BC

(19) JAPANESE PATENT OFFICE (JP)
(12) Official Gazette of Laid-Open Patent Applications (A)
(11) Japanese Laid-Open Patent Application Publication
(Kokai) No. 2000-124895
(P2000-124895A)
(43) Publication Date: 28 April 2000 (2000.4.28)

(51) Int. Cl.[7]:	ID Code:	FI	Theme code (for reference):
H04L 9/32		H04L 9/00	675A 5B089
G06F 13/00	354	G06F 13/00	345Z 5J104
G09C 1/00	660	G09C 1/00	660E
			660B
5/00		5/00	
H04L 9/08		H04L 9/00	601A
			601E

Request for Examination: Not Requested
Number of Claims: 3
OL (Total of 13 pages)

(21) Patent Application No.: H10-293827

(22) Filing Date: 15 October 1998 (1998.10.15)

(71) Applicant: 000002185
Sony Corporation
7-35 Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
(72) Inventor: Yoshito Ishibashi
c/o Sony Corporation
7-35 Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
(72) Inventor: Yoshitomo Osawa
c/o Sony Corporation
7-35 Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
(72) Inventor: Takeo Oishi
c/o Sony Corporation
7-35 Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
(72) Inventor: Tomoyuki Asano
c/o Sony Corporation
7-35 Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo
(74) Agent: 100082131
Patent Attorney, Yoshio Inamoto

F Terms (For Reference)
5B089 GA00 JA00 JA33 JB05 KA17
KB12 KB13 KC58 KH30
5J104 AA16 EA18 NA02 NA03 NA12
NA35 NA37 PA07 PA14

(54) [Title of the Invention] Information processing apparatus and method, and providing medium

(57) [Abstract]

[Problem] To prevent the key used for encrypting information from being read when the information is decrypted.

[Solving Means] A cross-authentication module 71 performs cross-authentication with an expanding portion 63 and generates a temporary key, a storage module 73 stores a second key, a decryption unit 91 decrypts a first key with the second key, and an encryption unit 92 encrypts the first key with the temporary key. A cross-authentication module 75 performs cross-authentication with storage means and generates a temporary key, a decryption module 76 decrypts a first key with the temporary key, and a decryption module 77 decrypts information with the first key.

51 RECEIVER
COMMUNICATING PORTION 61
CROSS-AUTHENTICATION MODULE 71
FEE MODULE 72
STORAGE MODULE 73
DECRYPTION/ENCRYPTION MODULE 74
DECRYPTION UNIT 91
ENCRYPTION MODULE 93
RANDOM NUMBER GENERATING UNIT 92
EXPANSION PORTION 63
CROSS-AUTHENTICATION MODULE 75
DECRYPTION MODULE 76
DECRYPTION MODULE 77
EXPANSION MODULE 78
WATERMARKING MODULE 79
IC CARD INTERFACE 64
IC CARD 55
CROSS-AUTHENTICATION MODULE 80
STORAGE MODULE 81
RECORDER 53
RECORDING/REPRODUCING PORTION 65
SAM 66
EXPANDING PORTION 67
MD DRIVER 54
USER HOME NETWORK 5

[Claims]

[Claim 1] An information processing apparatus comprising first storage means and first decryption means that use encrypted information, an encrypted first key for decrypting said information, and a second key for decrypting said first key to decrypt said information, characterized by

said first storage means comprising:

first cross-authentication means for performing cross-authentication with said first decryption means and generating a temporary key;

second storage means for storing said second key;

second decryption means for decrypting said first key with said second key; and

encryption means for encrypting said first key with said temporary key, and

said first decryption means comprising:

second cross-authentication means for performing cross-authentication with said first storage means and generating a temporary key;

third decryption means for decrypting said first key with said temporary key; and

fourth decryption means for decrypting said information with said first key.

[Claim 2] An information processing method for an information processing apparatus comprising storage means and decryption means that use encrypted information, an encrypted first key for decrypting said information, and a second key for decrypting said first key to decrypt said information, characterized by

said storage means executing:

a first cross-authentication step of cross-authentication with said decryption means and generation of a temporary key;

a storage step of storing said second key;

a first decryption step of decrypting said first key with said second key; and

an encryption step of encrypting said first key with said temporary key, and

said decryption means executing:

a second cross-authentication step of cross-authentication with said storage means and generation of a temporary key;

a second decryption step of decrypting said first key with said temporary key; and

a third decryption step of decrypting said information with said first key.

[Claim 3] A providing medium for an information processing apparatus comprising storage means and decryption means that use encrypted information, an encrypted first key for decrypting said information, and a second key for decrypting said first key to decrypt said information, characterized by provision of a computer-readable program that causes said storage means to execute a processing comprising:

a first cross-authentication step of cross-authentication with said decryption means and generation of a temporary key;

a storage step of storing said second key;

a first decryption step of decrypting said first key with said second key; and

an encryption step of encrypting said first key with said temporary key, and

that causes said decryption means to execute a processing comprising:

a second cross-authentication step of cross-authentication with said storage means and generation of a temporary key;

a second decryption step of decrypting said first key with said temporary key; and

a third decryption step of decrypting said information with said first key.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention] The present invention relates to an information processing apparatus and method, and a providing medium, and more particularly relates to an information processing

apparatus and method and providing medium for decrypting encrypted information.

[0002]

[Prior Art] A system based on information such as music being encrypted and transmitted to an information processing apparatus belonging to a user who has entered into a predetermined agreement who uses the information processing apparatus to decrypt and reproduce the information is available. In this system, a key used to encrypt the information is additionally encrypted with a predetermined key and recorded. The key used to encrypt the key for encrypting the information is stored in a storage medium for which improper access is difficult, and it is read and utilized only when the information is to be decrypted. Accordingly, the key used to encrypt the information cannot be improperly utilized and, in turn, the information cannot be improperly utilized.

[0003]

[Problems to be Solved by the Invention] However, when the information is decrypted, the key used to encrypt the information is decrypted and transmitted to a decryption circuit or a decryption apparatus for decrypting information. The key used to encrypt the information is in its decrypted state at this time and, as a result, it is able to be read comparatively easily from the communications either from within the apparatuses or between apparatuses and, if this key is read, the information is able to be improperly utilized without difficulty.

[0004] With the foregoing conditions in mind, it is an object of the present invention to prevent the key used for encrypting information from being read when the information is decrypted.

[0005] [Means of Resolving the Problems] The information processing apparatus according to claim 1 is characterized in that first storage means comprise first cross-authentication means for performing cross-authentication with first decryption means and

generating a temporary key, second storage means for storing a second key, second decryption means for decrypting a first key with the second key, and encryption means for encrypting the first key with the temporary key, and in that first decryption means comprise second cross-authentication means for performing cross-authentication with first storage means and generating a temporary key, third decryption means for decrypting a first key with the temporary key, and fourth decryption means for decrypting information with the first key.

[0006] The information processing method according to claim 2 is characterized in that storage means execute a first cross-authentication step for performing cross-authentication with decryption means and generating a temporary key, a storage step for storing a second key, a first decryption step for decrypting a first key with the second key, and an encryption step for encrypting the first key with the temporary key, and in that decryption means execute a second cross-authentication step for performing cross-authentication with storage means and generating a temporary key, a second decryption step for decrypting a first key with the temporary key, and a third decryption step for decrypting information with the first key.

[0007] The providing medium according to claim 3 is characterized by provision of a computer-readable program that causes storage means to execute a processing comprising a first cross-authentication step of cross-authentication with the decryption means and generation of a temporary key, a storage step of storing a second key, a first decryption step of decrypting the first key with the second key, and an encryption step of encrypting the first key with the temporary key, and that causes decryption means to execute a processing comprising a second cross-authentication step of cross-authentication with the storage means and generation of a temporary key, a second decryption step of decrypting the first key with

the temporary key, and a third decryption step of decrypting the information with the first key.

[0008] The information processing apparatus according to claim 1, information processing method according to claim 2 and providing medium according to claim 3 are used to perform cross-authentication, generate a temporary key, store a second key, decrypt a first key with the second key, encrypt the first key with the temporary key, decrypt the first key with the temporary key, and decrypt information with the first key.

[0009]

[Embodiments of the Invention] While the present invention is hereinafter described with reference to embodiments thereof, to ensure clarity of the corresponding relationship between the embodiments and the various means of the invention described in the claims, the characterizing features of the present invention are described below with the corresponding embodiment (a single example) indicated in parentheses following the means. However, this description should not be taken to mean the present invention is restricted to these means.

[0010] That is to say, the information processing apparatus according to claim 1 is characterized in that first storage means (for example, SAM 62 of FIG. 10) comprises first cross-authentication means (for example, cross-authentication module 71 of FIG. 10) for performing cross-authentication with first decryption means and generating a temporary key, second storage means (for example, storage module 73 of FIG. 10) for storing a second key, second decryption means (for example, decryption unit 91 of FIG. 10) for decrypting a first key with the second key, and encryption means (for example, encryption unit 92 of FIG. 10) for encrypting the first key with the temporary key, and in that first decryption means (for example, expanding portion 63 of FIG. 10) comprises second cross-authentication means (for example, cross-authentication module 75 of FIG. 10) for performing cross-

authentication with first storage means and generating a temporary key, third decryption means (for example, decryption module 76 of FIG. 10) for decrypting a first key with the temporary key, and fourth decryption means (for example, decryption module 77 of FIG. 10) for decrypting information with the first key.

[0011] FIG. 1 illustrates an EMD (Electronic Music Distribution) system in which the present invention has application. The content delivered to a user in a system of this kind is digital data of which the information itself has a value and, as an example thereof, music data will be hereinafter described. An EMD service centre 1 performs processings for sending a delivery key Kd to a content provider 2 and a user home network 5, receiving fee information and the like from the user home network 5 in accordance with the content used, calculating usage fees, and distributing profit distribution to the content provider 2 and the service provider 3.

[0012] The content provider 2, which possesses the digitalized content, inserts a watermark (electronic watermark) that identifies the content as its own, compresses and encrypts the content, and appends predetermined information thereto and sends the content to the service provider 3.

[0013] The service provider 3 appends a price to the content supplied from the content provider 2 and sends this to the user home network 5 through a network 4 constituted from, for example, a private cable network, the Internet, or a communications satellite.

[0014] The user home network 5 acquires the content transmitted with price appended from the service provider 3 and, together with decrypting the content for reproduction, executes a fee processing. The fee information obtained by the fee processing is transmitted to the EMD service centre 1 when the user home network 5 acquires a delivery key Kd from the EMD service centre 1.

[0015] FIG. 2 is a block diagram showing the functional configuration of the EMD service centre 1. A service provider managing portion 11 supplies profit distribution information to the service provider 3, and sends a delivery key Kd to the service provider 3 when information (usage policy) appended to the content supplied from the content provider 2 is encrypted. A content provider managing portion 12 sends a delivery key Kd and supplies profit distribution information to the content provider 2. A copyright managing portion 13 sends information expressing the content usage record by the user home network 5 to a copyright management body, for example, to JASRAC (Japanese Society for Rights of Authors, Composers and Publishers). A key server 14 stores the delivery key Kd and supplies it to the content provider 2 or the user home network 5 or the like via the content provider managing portion 12 or a user managing portion 18. The user managing portion 18 stores fee information which is information that expresses the content usage record of the user home network 5, pricing information corresponding to this content, and the usage policy corresponding to this content input thereto in a log data managing portion 15.

[0016] An example of a delivery key Kd being regularly transmitted from the EMD service centre 1 to a receiver 51 (described later with reference to FIG. 10) configured from a user home network 5 and a content provider 2 will be hereinafter described with reference to FIGS. 3 to 6. FIG. 3 shows the delivery key Kd possessed by the EMD service centre 1, the delivery key Kd possessed by the content provider 2 and the delivery key Kd possessed by the receiver 51 in January 1998 when the content is initially provided by the content provider 2 and initially used by the receiver 51 comprising the user home network 5.

[0017] In the example of FIG. 3, a delivery key Kd is usable from the first day to the last day of a calendar month, for example, a version 1 delivery key Kd with a

random number value "aaaaaaaa" of a predetermined number of bits is usable from January 1, 1998 to January 31, 1998 (that is to say, a content key Kco for encrypting the content distributed by the service provider 3 to the user home network 5 in the period from January 1, 1998 to January 31, 1998 is encrypted with the version 1 delivery key Kd). A version 2 delivery key Kd with a random number value "bbbbbbbb" of a predetermined number of bits is usable from February 1, 1998 to February 28, 1998 (that is to say, a content key Kco for encrypting the content distributed by the service provider 3 to the user home network 5 during the given period is encrypted by the version 2 delivery key Kd). Similarly, a version 3 delivery key Kd is usable during March 1998, a version 4 delivery key Kd is usable during April 1998, a version 5 delivery key Kd is usable during May 1998, and a version 6 delivery key Kd is usable during June 1998.

[0018] Prior to the content provider 2 beginning to provide the content, the EMD service centre 1 sends six delivery keys Kd - versions 1 to 6 - usable from January 1998 to June 1998 to the content provider 2, and the content provider 2 receives and stores these six delivery keys Kd. The reason for storing a 6-month period of delivery keys Kd is because, prior to the provision of content, a predetermined period of time is required for the content provider 2 to carry out preparations such as content and content key encryption.

[0019] Prior to the receiver 51 beginning to use the content, the EMD service centre 1 sends three delivery keys Kd - versions 1 to 3 - usable from January 1998 to March 1998 to the receiver 51, and the receiver 51 receives and stores these three delivery keys Kd. The reason for storing a 3-month period of delivery keys Kd is to avoid a situation in which, regardless of the content being used during the valid agreement period, the content cannot be used due to trouble caused by the

receiver 51 being unable to be connected to the EMD service centre 1, as well as to decrease the frequency of connections to the EMD service centre 1 to reduce the load on the user home network 5.

[0020] The version 1 delivery key Kd is used by the EMD service centre 1, the content provider 2, and the receiver 51 from which the user home network 5 is constituted during the period from January 1, 1998 to January 31, 1998.

[0021] The transmission of delivery keys Kd from the EMD service centre 1 to the content provider 2 and the receiver 51 on February 1, 1998 will be described with reference to FIG. 4. The EMD service centre 1 sends six delivery keys Kd - versions 2 to 7 - usable from February 1998 to July 1998 to the content provider 2, and the content provider 2, having received the six delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery keys Kd. The EMD service centre 1 sends three delivery keys Kd - versions 2 to 4 - usable from February 1998 to April 1998 to the receiver 51, and the receiver 51, having received the three delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery keys Kd. The EMD service centre 1 stores the version 1 delivery key Kd without alteration. This is to ensure previously used delivery keys Kd can be utilized in the event of unforeseen trouble occurring, or an illegal act being committed or detected.

[0022] The version 2 delivery key Kd is used by the EMD service centre 1, the content provider 2, and the receiver 51 from which the user home network 5 is constituted during the period from February 1, 1998 to February 28, 1998.

[0023] The transmission of delivery keys Kd from the EMD service centre 1 to the content provider 2 and the receiver 51 on March 1, 1998 will be described with reference to FIG. 6. The EMD service centre 1 sends six delivery keys Kd - versions 3 to 8 - usable from March

1998 to August 1998 to the content provider 2, and the content provider 2, having received the six delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery keys Kd. The EMD service centre 1 sends three delivery keys Kd - versions 3 to 5 - usable from March 1998 to May 1998 to the receiver 51, and the receiver 51, having received the three delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery keys Kd. The EMD service centre 1 stores the version 1 delivery key Kd and the version 2 delivery key without alteration.

[0024] The version 3 delivery key Kd is used by the EMD service centre 1, the content provider 2, and the receiver 51 from which the user home network 5 is constituted during the period from March 1, 1998 to March 31, 1998.

[0025] The transmission of delivery keys Kd from the EMD service centre 1 to the content provider 2 and the receiver 51 on April 1, 1998 will be described with reference to FIG. 6. The EMD service centre 1 sends six delivery keys Kd - versions 4 to 9 - usable from April 1998 to September 1998 to the content provider 2, and the content provider 2, having received the six delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery keys Kd. The EMD service centre 1 sends three delivery keys Kd - versions 4 to 6 - usable from April 1998 to June 1998 to the receiver 51, and the receiver 51, having received the three delivery keys Kd, overwrites the previously received and stored delivery keys Kd and stores the new delivery key Kd. The EMD service centre 1 stores the version 1 delivery key Kd, the version 2 delivery key, and the version 3 delivery key without alteration.

[0026] The version 4 delivery key Kd is utilized by the EMD service centre 1, the content provider 2, and the receiver 51 from which the user home network 5 is

constituted during the period from April 1, 1998 to April 30, 1998.

[0027] Distributing delivery keys Kd several months in advance in this way allows a user to make a content purchase even despite them not having accessed the EMD service centre 1 at all for a month or two, and to access the EMD service centre 1 and receive keys at a convenient later time.

[0028] A profit distribution portion 16 computes the profits to be shared by the EMD service centre 1, the content provider 2 and the service provider 3 according to the fee information, pricing information and usage policy supplied from the log data managing portion 15. A cross-authenticating portion 17 performs a later-described cross-authentication with the content provider 2, service provider 3, and user home network 5 device.

[0029] The user managing portion 18 possesses a user registration database and, when a registration request is received from a user home network 5 device, executes a processing such as a search of the user registration database and, in response to the recorded details therein, registration or registration refusal of the device. When the user home network 5 is configured from a plurality of devices possessing a function that facilitates connection with the EMD service centre 1, the user managing portion 18 designates the device for which a settlement is to be performed in accordance with the result of a judgment processing result as to whether or not registration thereof is possible, and, furthermore, sends a registration list which prescribes the usage conditions to the predetermined device of the user home network 5.

[0030] In the example user registration database shown in FIG. 7, ID (Identification Data) constituted from 64 bits peculiar to the user home network 5 device is recorded therein and, correspondent to this ID (that is to say, to each device with this ID), information such as whether settlement processing is possible,

registration is possible, and connection with the EMD service centre 1 is possible is recorded therein. The information stored in the user registration database as to whether registration is possible is updated in a predetermined time period on the basis of information including non-payment of fees and improper processing and so on supplied from an approved institution (for example, a bank) or the service provider 3. The user managing portion 18 refuses registration when the registration request is from a device with an ID for which registration is recorded as being disapproved, and the device for which registration has been refused is thereafter unable to used the content of the system.

[0031] Information as to whether or not a settlement processing is possible recorded in the user registration database expresses whether or not settlement using this particular device is possible. When the user home network 5 is constituted from a plurality of devices for which uses including content playback and copy are possible, a single piece of device thereof for which settlement is possible outputs the fee information, pricing information and usage policy of all devices of the user home network 5 registered in the EMD service centre 1 to the EMD service centre 1. Information as to whether connection with the EMD service centre 1 is possible recorded in the user registration database expresses whether or not a piece of device is able to be connected to the EMD service centre 1, and a device registered as being connectable therewith outputs fee information to the EMD service centre 1 via other devices of the user home network 5.

[0032] In addition, fee information, pricing information and usage policy are supplied from the device of the user home network 5 to the user managing portion 18 which outputs this information to the log data managing portion 15 and, furthermore, supplies delivery keys Kd to the user home network 5 by a predetermined processing (timing).

[0033] A billing portion 19 computes the user fee based on, for example, the fee information, pricing information and usage policy supplied from the log data managing portion 15, and supplies the result thereof to an accounting portion 20. The casher portion 20 executes a settlement processing in communication with an external bank or the like (not shown in the diagram) on the basis of the usage fee amount to be paid or charged to the user, the content provider 2, and the service provider 3. An auditing portion 21 carries out a propriety audit (that is, checks for any illegality) of the fee information, pricing information and usage policy supplied from the device in the user home network 5.

[0034] FIG. 8 is a block diagram showing a functional configuration of the content provider 2. A content server 31 stores the content to be supplied to the user, and supplies this content to a watermarking portion 32. The watermarking portion 32 appends a watermark to the content supplied by the content server 31 and supplies this to a compressing portion 33. The compressing portion 33 compresses the content supplied by the watermarking portion 32 by an ATRAC2 (Adaptive Transform Acoustic Coding 2) (Trademark) or similar method, and supplies this to an encrypting portion 34. The encrypting portion 34 encrypts the content compressed by the compressing portion 33 by common-key cryptography such as DES (Data Encryption Standard) using a random number supplied by a random number generating portion 35 as a key (hereinafter this random number is referred to as a content key Kco), and outputs the result thereof to a secure container producing portion 38.

[0035] The random number generating portion 35 supplies a random number of a predetermined number of bits for use as a content key Kco to the encrypting portion 34 and the encrypting portion 36. The encrypting portion 36 uses common-key cryptography such as DES to encrypt the content key Kco with the delivery key Kd supplied

from the EMD service centre 1, and outputs the result thereof to the secure container producing portion 38.

[0036] DES is an encryption method that employs a 56-bit common key to process 64-bit blocks of plain text as a single block. DES processing comprises a section (data mixing portion) for mixing plain text and converting it to cipher text, and a section (key processing portion) for generating a key (expansion key) from a common key for use by the data mixing portion. All algorithms of a DES are publicly accessible and, accordingly, the basic processing executed by the data mixing portion will be hereinafter described in brief.

[0037] First, 64 bits of plain text are divided into high-order 32 bits H_0 and low-order 32 bits L_0. The input of a 48-bit expansion key K_1 supplied from the key processing portion and the low-order 32 bits L_0 is assumed, and the output of an F function obtained by mixing the low-order 32 bits L_0 is computed. The F function is constituted from two fundamental types of conversion, namely "substitution" in which numeric values are substituted according to a prescribed rule, and "transposition" in which bit positions are transposed according to a prescribed rule. The high-order 32 bits H_0 are subject to an exclusive OR operation with the output from the F function, and the result thereof is denoted as L_1. L_0 is denoted as H_1.

[0038] This processing is iterated 16 times on the basis of the high-order 32 bits H_0 and the low-order 32 bits L_0, and the thus-obtained high-order 32 bits H_{16} and low-order 32 bits L_{16} are output as cipher text. For decryption, the routine described above is reversed using a common key used for the encryption.

[0039] A policy storing portion 37 stores the content usage policy, and outputs the usage policy correspondent to the content to be encrypted to the secure container producing portion 38. The secure container producing portion 38 prepares a content provider secure container constituted from encrypted

content, an encrypted content key Kco, a usage policy, a signature produced using a hash value of the encrypted content, encrypted content key Kco and usage policy and, furthermore, a certificate containing a public key Kpcp of the content provider 2, and supplies this content provider secure container to the service provider 3. A cross-authenticating portion 39 performs cross-authentication with the EMD service centre 1 prior to a delivery key Kd being received from the EMD service centre 1 and, in addition, performs cross-authentication with the service provider 3 prior to the content provider secure container being transmitted to the service provider 3.

[0040] The signature, which is appended to data or to a later-described certificate, constitutes data used for checking for falsification and authenticating the author, and is produced by obtaining a hash value using a hash function on the basis of the data which is to be sent, and encrypting this hash value with a public-key cryptography secret key.

[0041] Hash function and signature verification will be hereinafter described. A hash function constitutes a function that assumes predetermined data to be transmitted has been input which compresses this data to data of a specific bit length, and outputs this as a hash value. The characterizing features of a hash function are that prediction of input from a hash value (output) is difficult, most bits of a hash value change when one bit of data input on a hash function changes, and determining whether input data has the same hash value is difficult.

[0042] The receiver in receipt of a signature and data decrypts the signature with a public-key cryptography public key, and obtains a resultant value (hash value). The hash value of the received data is then calculated, and a judgment of whether the calculated hash value is equal to the hash value obtained by decrypting the signature is carried out. Where the hash value of the received data is judged to be equal to the decrypted

hash value, this indicates that the received data has not been falsified and is data that has been transmitted from a sender in possession of the secret key corresponding to the public key. Examples of hash functions used for signatures include MD4, MD5 and SHA-1.

[0043] Public-key cryptography will be hereinafter described. In contrast to common-key cryptography which uses the same key (a common key) for encryption and decryption, in public-key cryptography the key used for encryption and the key used for decryption differ. When public-key cryptography is employed, one of the keys is made public and the other key can be kept secret, and while the key that can be made public is called a public key the key that is kept secret is called a secret key.

[0044] A typical example of public-key cryptography is the RSA (Rivest-Shamir-Adleman) cipher that will be hereinafter described in brief. First, two sufficiently large prime numbers p and q are determined, and a product n thereof is determined. The least common multiple L of (p-1) and (q-1) is computed, and a number e equal to or greater than 3 and less than L and relatively prime to L is determined (that is to say, the only number that will go into both e and L is 1).

[0045] Next, a multiplicative inverse d of e is determined by modulo L arithmetic. In other words, the relationship ed=1 mod L is established between d, e, and L, where d can be computed using an Euclid algorithm. Here, n and e are public keys and p, q, and d are secret keys.

[0046] Cipher text C is computed from plain text M by the processing of equation (1).

$C=M^e \bmod n$ (1)

[0047] The cipher text C is decrypted into plain text M by the processing of equation (2).

$M=C^d \bmod n$ (2)

[0048] While a demonstration has been omitted, the reason why plain text is able to be converted into

cipher text using an RSA cipher and the cipher text can be decrypted is that the processing is based on Fermat's first theorem and, accordingly, equation (3) holds true:

$M=C^{d=}(M^{e})^{d=M.sup.ed=M} \bmod n$ (3)

[0049] While a user who knows the secret keys p and q can compute the secret key d from the public key e, if the number of digits of the public key n is increased to the extent that unique factorization of the public key n is difficult from the viewpoint of the quantity of computations, the secret key d cannot be computed from the public key e and, accordingly, the cipher text cannot be decrypted by awareness of the public key n alone. As described above, in RSA cryptography the key used for encryption is different to the key used for decryption.

[0050] As an example of another public-key cipher, an Elliptic Curve Cryptography system will be hereinafter described in brief. A point on an elliptic curve $y^{2=x.sup.3+ax+b}$ is taken as b. To define the addition of points on the elliptic curve, nB is taken to express a result obtained by n additions of B. Subtractions are similarly defined. Computation of n from B and Bn has been shown to be difficult. B and nB are taken as public keys, and n is taken as a secret key. Employing a random number r, cipher texts C1 and C2 are computed by computation based on the processing of equations (4) and (5) using public keys.

$C1=M+rnB$ (4) $C2=rB$ (5)

[0051] Cipher texts C1 and C2 are decrypted into plain text M by the processing of equation (6).

$M=C1-nC2$ (6)

[0052] Decryption is possible only when in possession of the secret key n. Similarly to the RSA cryptosystem as described above, in Elliptic Curve Cryptography the key for encryption and the key for decryption also differ.

[0053] FIG. 9 is a block diagram illustrating the functional configuration of the service provider 3. A

content server 41 stores the encrypted content supplied from the content provider 2, and supplies this to a secure container producing portion 44. A pricing portion 42 produces pricing information on the basis of the usage policy correspondent to the content, and supplies this to the secure container producing portion 44. A policy storing portion 43 stores the content usage policy supplied from the content provider 2 and supplies this to a secure container producing portion 44. The cross-authenticating portion 45, prior to receipt of the content provider secure container from the content provider 2, performs cross-authentication with the content provider 2 and, in addition, prior to transmitting the content provider secure container to the user home network 5, performs cross-authentication with the user home network 5. In addition, when the content provider 2 supplies the usage policy encrypted with a delivery key Kd, the cross-authenticating portion 45, prior to receipt of a delivery key Kd from the EMD service centre 1, performs cross-authentication with the EMD service centre 1.

[0054] FIG. 10 is a block diagram illustrating the configuration of the user home network 5. A receiver 51 receives a service provider secure container containing content from the service provider 3 via a network 4, and decrypts, expands and reproduces the content.

[0055] A communicating portion 61 communicates with the service provider 3 or the EMD service centre 1 via the network 4 receiving or sending predetermined information therewith. A SAM (Secure Application Module) 62 performs a cross-authentication with the service provider 3 or the EMD service centre 1, and decrypts the content cipher or encrypts the content and, furthermore, stores a delivery key Kd or the like. An expanding portion 63 decrypts the content cipher, expands this using an ATRAC2 system, and inserts a predetermined watermark in the content. An IC (Integrated Circuit) card interface 64 converts a signal from the IC card 55 to a predetermined format,

and outputs this to the IC card 55 loaded in the receiver 51 or converts a signal from the IC card 55 and outputs this to a SAM 62.

[0056] The SAM 62, which performs cross-authentication with the service provider 3 or EMD service centre 1, which executes fee processing, which decrypts and encrypts a content key Kco, and which stores predetermined data such as license usage conditions information and so on, is constituted from a cross-authentication module 71, a fee module 72, a storage module 73 and a decryption/encryption module 74. The SAM 62, which is constituted from single-chip ICs designed exclusively for cryptographic use, has as a multi-layer construction in which internal memory cells are sandwiched by dummy layers of aluminium and the like and, in addition, as it is operated across a small voltage or frequency range, it possesses a characteristic (tamperproofness) that ensures it is hard for data to be illegally read from the exterior.

[0057] The cross-authentication module 71 performs cross-authentication with the service provider 3 or the EMD service centre 1 and, in accordance with need, supplies a temporary key Ktemp (session key) to the encryption/decryption module 74. The fee module 72 generates license usage conditions information and fee information from the usage policy and pricing information (and in some cases usage control information) contained in the service provider 3, and outputs this to the storage module 73 or an HDD (Hard Disk Drive) 52. The storage module 73 stores data such as fee information and the delivery keys Kd and so on supplied from the fee module 72 or decryption/encryption module 74, and supplies data such as the delivery keys Kd when another functional block executes a predetermined processing.

[0058] The encryption/decryption module 74 is constituted from a decryption unit 91, a random number generation unit 92, and an encryption unit 93. The decryption unit 91 decrypts the encrypted content key

Kco with a delivery key Kd, and outputs the result to the encryption unit 93. The random number generation unit 92 generates a random number of a predetermined digit number, and outputs this as a save key Ksave to the encryption module 93 and the storage module 73. Notably, once this has been generated and saved, further need thereof is eliminated. The encryption unit 93 re-encrypts the decrypted content key Kco with the save key Ksave, and outputs the result to the HDD 52. When the encryption module 93 sends the content key Kco to the expanding portion 63, the encrypted content key Kco is encrypted with the temporary key Ktemp.

[0059] The expanding portion 63, which decrypts and expands the content and appends a predetermined watermark thereto, is constituted from the cross-authentication module 75, a decryption module 76, an expansion module 78, and a watermarking module 79. The cross-authentication module 75 performs cross-authentication with the SAM 62, and outputs a temporary key Ktemp to the decryption module 76. The decryption module 76 decrypts the content key Kco output from the storage module 73 and encrypted with the temporary key Ktemp with the temporary key Ktemp, and outputs the result to the decryption module 77. The decryption module 77 decrypts the content stored in the HDD 52 with the content key Kco, and outputs the result to the expansion module 78. The expansion module 78 further expands the decrypted content using a method such as ATRAC2 or the like, and outputs the result to the watermarking module 79. The watermarking module 79 inserts a predetermined watermark that identifies the receiver 51 in the content, and outputs this to a recorder 53, or outputs it to a speaker not shown in the diagram for reproducing the music.

[0060] The HDD 52 records the content supplied from the service provider 3. The recorder 53, which records and reproduces content supplied from the service provider 3 on a loaded optical disk (not shown in the diagram), is constituted from a recording/reproducing portion 65,

SAM 66 and expanding portion 67. The recording/reproducing portion 65, in which the optical disk is loaded, records content for reproduction on this optical disk. The SAM 66 has an identical function to the SAM 62 and, accordingly, a description thereof is omitted. The expanding portion 67 has an identical function to the expanding portion 63 and, accordingly, a description thereof is omitted. An MD (Mini Disk: Trademark) driver 54 records content for reproduction supplied from the service provider 3 on a loaded MD not shown in the diagram.

[0061] The IC card 55 loaded in the receiver 51 stores the delivery key Kd stored in the storage module 73 and predetermined data such as the ID of a device. For example, when a new receiver 51 is purchased and is to be used to replace a hitherto used receiver 51, first, the user stores predetermined data such as the delivery key Kd stored in the storage module 73 of the hitherto used receiver 51 in the IC card 55. Next, the user loads the IC card 55 in the new receiver 51, and operates the receiver 51 to register the new receiver 51 in the user managing portion 18 of the EMD service centre 1. The user managing portion 18 of the EMD service centre 1 searches the database held by the user managing portion 18 on the basis of data stored in the IC card 55 (ID and so on the hitherto used receiver 51) for the user name and credit card number used for payment of usage fees and, because the registration processing is executed on the basis of this data, the need for a user to carry out a troublesome task of inputting data is eliminated. The IC card 55 is constituted from a cross-authentication module 80 and a storage module 81. The cross-authentication module 80 performs cross-authentication with the SAM 62. The storage module 81, stores data supplied from the SAM 62 via the IC card interface 64, and outputs the stored data to the SAM 62.

[0062] FIG. 11 is a block diagram showing another example of the configuration of a user home network 5.

The receiver 51 and recorder 53 of this configuration describe a configuration from which the expanding portion 63 and expanding portion 67 shown in FIG. 10 have been omitted. Instead, a decoder 56 connected to the recorder 53 serves an identical function to the expanding portion 63 and the expanding portion 67. Other configurations are identical to those of FIG. 10.

[0063] The decoder 56, which decrypts and expands the content and appends a watermark thereto, is constituted from a cross-authentication module 101, a decryption module 102, a decryption module 103, an expansion module 104, and a watermarking module 105. The cross-authentication module 101 performs cross-authentication with the SAM 62 and a SAM 66, and outputs a temporary key Ktemp to the decryption module 102. The decryption module 102 uses the temporary key Ktemp to decrypt a content key Kco output from the SAM 62 and encrypted by the temporary key Ktemp, and outputs the result to the decryption module 103. The decryption module 103 decrypts the content recorded on the HDD 52 with the content key Kco, and outputs the result to the expansion module 104. The expansion module 104 further decompresses the decrypted content by a method such as ATRAC2, and outputs the result to the watermarking module 105. The watermarking module 105 inserts a predetermined watermark that identifies the decoder 56 into the content, and outputs the result to the recorder 53 or to speakers (not shown) to reproduce the music.

[0064] FIG. 12 is a diagram describing information transmitted and received between the EMD service centre 1, the content provider 2, the service provider 3 and the user home network 5. The content provider 2 stores encrypted content, an encrypted content key Kco, a usage policy and a signature in a content provider secure container (the details of which will be described later with reference to FIG. 13), and appends an authentication certificate (the details of which will be described later with reference to FIG. 14) of

the content provider 2 to the content provider secure container and sends this to the service provider 3. The content provider 2 also appends an authentication certificate of the content provider 2 to the usage policy and the signature and sends this to the EMD service centre 1.

[0065] The service provider 3 generates pricing information on the basis of a usage policy contained in the received content provider secure container, stores the encrypted content, the encrypted content key Kco, the usage policy, the pricing information and the signature in the service provider secure container (the details of which will be described later with reference to FIG. 15), and appends an authentication certificate of the service provider 3 (the details of which will be described later with reference to FIG. 16) to the service provider secure container and sends this to the user home network 5. The service provider 3 also appends an authentication certificate of the service provider 3 to the pricing information and signature and sends this to the EMD service centre 1.

[0066] The user home network 5 generates license use information from the usage policy contained in the received provider secure container, and uses the content in accordance with this license use information. When the content key Kco is decrypted in the user home network 5, fee information is generated. This fee information is encrypted at a predetermined timing, and is transmitted to the EMD service centre 1 with a usage policy and a signature appended thereto.

[0067] The EMD service centre 1 computes the usage fee on the basis of this fee information and the usage policy, and calculates the profit to be shared between the EMD service centre 1, the content provider 2, and the service provider 3. The EMD service centre 1 compares the usage policy received from the content provider 2, the pricing information received from the service provider 3 and the fee information and usage policy received from the user home network 5, and

carries out an audit to determine whether any illegality such as falsification of usage policy or appending of an improper price has been performed either by the service provider 3 or the user home network 5.

[0068] FIG. 13 is a diagram describing the content provider secure container. The content provider secure container contains content encrypted with a content key Kco, a content key Kco encrypted with a delivery key Kd, a usage policy and a signature. The signature constitutes data obtained by encrypting a hash value generated by application of a hash function to the content encrypted with the content key Kco, the content key Kco encrypted with the delivery key Kd, and the usage policy with a secret key Kscp of the content provider 2.

[0069] FIG. 14 is a diagram describing the authentication certificate of the content provider 2. The authentication certificate of the content provider 2 contains the version no. of the authentication certificate, the serial no. of the authentication certificate assigned to the content provider 2 by a certifying agency, algorithms and parameters employed in the signature, the name of the certifying agency, the period of validity of the authentication certificate, the name of the content provider 2, the public key Kpcp of the content provider, and the signature. The signature constitutes data obtained by encrypting a hash value generated by application of a hash function on the version no. of the certificate, the serial no. of the authentication certificate assigned to the content provider 2, the algorithm and parameters employed for the signature, the name of the certifying agency, the period of validity of the authentication certificate, the name of the content provider 2, and the public key Kpcp of the content provider with a secret key Ksca of the authenticating agency.

[0070] FIG. 15 is a diagram describing the service provider secure container. The service provider secure container contains content encrypted with a content key Kco, a content key Kco encrypted with a delivery key Kd, usage policy, pricing information and a signature. The signature constitutes data obtained by encrypting a hash value generated by application of a hash function on the content encrypted with the content key Kco, the content key Kco encrypted with the delivery key Kd, the usage policy and the pricing information with a secret key Kssp of the service provider 3.

[0071] FIG. 16 is a diagram describing the authentication certificate of the service provider 3. The authentication certificate of the service provider 3 contains the version no. of the certificate, the serial no. of the authentication certificate assigned to the service provider 3 by the certifying agency, algorithms and parameters employed in the signature, the name of the certifying agency, the period of validity of the authentication certificate, the name of the service provider 3, the public key Kpsp of the service provider, and a signature. The signature constitutes data obtained by encrypting a hash value generated by application of a hash function on the version no. of the certificate, the serial no. of the authentication certificate assigned to the service provider 3, the algorithm and parameters employed for the signature, the name of the certifying agency, the period of validity of the authentication certificate, the name of the service provider 3, and the public key Kpsp of the service provider with a secret key Ksca of the authenticating agency.

[0072] FIG. 17 is a diagram illustrating the usage policy, pricing information, and license usage conditions information. The usage policy (FIG. 17(A)) possessed by the content provider 2 is prepared for each content and indicates the usage details usable by the user home network 5. For example, the usage policy of FIG. 17(A) shows that while the user home network 5

is licensed for reproduction and multiple copy of the content, it is not licensed for a single copy.

[0073] FIG. 18 is a diagram describing single copy and multiple copy. Multiple copy refers to the case where license usage conditions for content for which a copy license has been assigned to the license usage conditions information are purchased, and a plurality of copies are produced from this content. However, as shown in FIG. 18(A), further copy thereof is prohibited (not licensed). Single copy refers to the case where license usage conditions for content for which a copy license has been assigned to the license usage conditions information are purchased, and just a single copy is produced from this content. For single copy as well, as shown in FIG. 18(B), further copying of this copy is prohibited (not licensed).

[0074] As shown in FIG. 17(B), the service provider 3 adds pricing information from the content provider 2 to the usage policy (FIG. 17(A)). For example, the pricing information of FIG. 17(B) indicates a 150¥ fee for reproducing the content, and an 80¥ usage fee for the multiple copy use thereof. While not shown in FIG. 17, single copy pricing information expresses a usage fee per copy and, for example, the usage fee paid for 3 copies is three times the usage fee paid for a single copy. Content for multiple copy or single copy licensing is limited to content for which a copy license according to license usage conditions inform ation has been assigned for which license usage conditions have been purchased.

[0075] The user home network 5 stores the usage details indicating the license usage conditions information (FIG. 17(C)) selected by a user from the usable usage details (FIG. 17(B) indicating the usage policy supplied from the service provider 3. For example, the license usage conditions information of FIG. 17(C) indicate that the content can be reproduced, and that single copy and multiple copy are prohibited.

[0076] FIG. 19 is a diagram describing the usage policy and pricing information where, compared to FIG. 17, the content provider 2 has added profit distribution information to the usage policy, and the service provider 3 has assigned profit distribution information to the pricing information. In contrast to the example shown in FIG. 17, in the example of FIG. 19, supplementary information indicating a profit for the content provider 2 of 70¥ when the content is reproduced and 40¥ when used for multiple copy is provided (FIG. 19(A)). Furthermore, supplementary profit distribution information indicating that the profit for the service provider 3 is 60¥ when the content is reproduced and 30¥ when used for multiple copy is provided (FIG. 19(B). The price, similarly to the case of FIG. 17(A), is 150¥ for reproduction and 40¥ for multiple copy. The amount (for example 20¥) obtained by subtracting the profit of the content provider 2 (for example 70¥) and the profit of the service provider 3 (for example 60¥) from the price (for example 150¥) represents the profit of the EMD service centre 1. The EMD service centre 1 is able to compute the profits of each of the content provider 2, the service provider 3 and the EMD service centre 1 by obtaining the usage policy, the profit distribution ratio and pricing information via the user home network 5 together with fee information (FIG. 19(C)) which expresses the content usage record of the user home network 5.

[0077] FIG. 20 is a diagram describing the usage policy, pricing information and license usage conditions information when a plurality of modes are set for reproducing the content. In the example of FIG. 20(A), unrestricted reproduction, frequency restricted (in this case 5x) reproduction, and date restricted (in this case until December 31, 1998) reproduction are set by the service provider 3 as the usage policy and pricing information for reproducing the content. Where a user selects 5x frequency restricted reproduction of

the content, in a state in which the content has been received but not yet reproduced, "5" is recorded as the value correspondent to the frequency restriction of the license usage conditions information of the user home network 5 as shown in FIG. 20B. The value correspondent to this frequency restriction is decremented in the user home network 5 every time the content is reproduced (used) and, for example, after being reproduced 3x, the value has decremented to "2" as shown in FIG. 20(C). When the value correspondent to the frequency restriction is "0", the user home network 5 is no longer able to use the content for reproduction.

[0078] FIG. 21 is a diagram describing another example of information transmitted and received between the EMD service centre 1, the content provider 2, the service provider 3 and the user home network 5. In contrast to the example shown in FIG. 12, in the example shown in FIG. 21 the service provider 3 produces usage control information on the basis of the usage policy from the content provider 2. The usage control information is stored with the content and so on in a service provider secure container, transmitted to the user home network 5, and also transmitted to the EMD service centre 1. The usage control information is also transmitted from the user home network 5 to the EMD service centre 1 together with the fee information and usage policy.

[0079] FIG. 22 is a diagram describing the service provider secure container of the example of FIG. 21. the service provider secure container contains content encrypted with a content key Kco, a content key Kco encrypted with a delivery key KD, a usage policy, usage control information, pricing information and a signature. The signature constitutes data obtained by encrypting a hash value generated by application of a hash function on the content key Kco, the content key Kco encrypted with a delivery key KD, the usage policy, the usage control information, the pricing information

and the signature with a secret key Kssp of the service provider 3.

[0080] FIG. 23 is a diagram illustrating the configuration of the usage policy, usage control information, pricing information and license usage conditions of the example of FIG. 21. In the example shown in FIG. 23, the usage policy (FIG. 23(A)) of the content provider 2, despite pricing information being appended without alteration, is not of a format that enables comparative reference of pricing information with usage policy. Thereupon, the service provider 3 generates usage control information of a format that enables comparative reference of pricing information with pricing information on the basis of the usage policy thereof, appends the pricing information thereto, and sends this to the user home network 5 (FIG. 23(B)). License usage conditions information (FIG. 23(C)) is generated in the user home network from this transmitted information. The content provider 2 of FIG. 23 is advantageous in that a usage policy of smaller data quantity than required for the case described in FIG. 12 may be recorded.

[0081] FIG. 24 is a diagram describing a further configuration of the content and information appended to the content transmitted and received between the EMD service centre 1, the content provider 2, the service provider 3 and the user home network 5. In contrast to the example shown in FIG. 21, in the example of FIG. 24 the usage policy, the usage control information, the pricing information and the fee information are encrypted and transmitted using a public key cipher. The system of FIG. 24 has comparatively better safety than the example of FIG. 21 with respect to external system attack.

[0082] FIG. 25 is an example for describing the content provider secure container of the example of FIG. 24. The content provider secure container contains content encrypted with a content key Kco, a content key Kco encrypted with a delivery key Kd, usage policy

encrypted with a delivery key Kd, and a signature. The signature constitutes data obtained by encoding a hash value generated by application of a hash function on the content encrypted with a content key Kco, the content key Kco encrypted with a delivery key Kd, and the usage policy encrypted with a delivery key Kd with a secret key Kscp of the content provider 2.

[0083] FIG. 26 is a diagram describing the service provider secure container of the example of FIG. 24. The service provider secure container contains content encrypted with a content key Kco, a content key Kco encrypted with a delivery key Kd, a usage policy encrypted with a delivery key Kd, usage control information encrypted with a delivery key Kd, pricing information encrypted with a delivery key Kd, and a signature. The signature constitutes data obtained by encoding a hash value generated by application of a hash function on the content key Kco, the content key Kco encrypted with the delivery key Kd, the usage policy encrypted with a delivery key Kd, the usage control information encrypted with a delivery key Kd, and the pricing information encrypted with a delivery key Kd with a secret key Kssp of the service provider 3.

[0084] FIG. 27 is a diagram describing the operation when the EMD service centre 1 receives fee information from the user home network 5. Subsequent to cross-authentication with the user home network 5, the user managing portion 18 produces a shared temporary key Ktemp, and encrypts a delivery key Kd from a key server 14 with this key and sends the result to the user home network 5. The user home network 5, subsequent to decrypting the received delivery key Kd with the shared temporary key Ktemp, updates the delivery key Kd in accordance with need. In addition, employing the shared temporary key Ktemp, it encrypts the fee information and usage policy and so on and sends the result thereof to the EMD service centre 1. This is received by the user managing portion 18. The user managing portion 18,

subsequent to decrypting the received fee information and usage policy and so on with the shared temporary key Ktemp, sends the result thereof to a log data managing portion 15 and a billing portion 19. The log data managing portion 15, having judged that a settlement is to be executed, sends the received fee information to the profit distribution portion 16 and, furthermore, sends the received fee information and usage policy and so on to the billing portion 19. The profit distribution portion 16 computes the billing amount and paid amount for the content provider 2, the service provider 3 and EMD service centre 1 itself. The billing portion 19 computes the amount paid by a user and sends this information to an accounting portion 20. The accounting portion 20 executes a settlement processing in communication with an external bank or the like not shown in the diagram. At this time, if usage fee non-payment information or the like exists, this information is transmitted to the billing portion 19 and the user managing portion 18 where it can be used for reference for subsequent user registration processing and delivery key Kd send processing.

[0085] FIG. 28 is a diagram describing the profit distribution processing operation of the EMD service centre 1. The log data managing portion 15 sends fee information that indicates a user content usage record, usage policy and pricing data to the profit distribution portion 16. The profit distribution portion 16 computes the profits of each of the content provider 2, the service provider 3 and the EMD service centre 1 on the basis of this information, and sends the result thereof to a service provider managing portion 11, a content provider managing portion 12, the accounting portion 20 and a copyright managing portion 13. The accounting portion 20 executes a settlement processing in communication with an external bank or the like not shown in the diagram. The service provider managing portion 11 sends the profit information of the service provider 3 to the service provider 3. The

content provider managing portion 12 sends the profit information of the content provider 2 to the content provider 2. An auditing portion 21 carries out a propriety audit of the fee information, pricing information and usage policy supplied from the device of the user home network 5.

[0086] FIG. 29 is a diagram describing the processing operation for sending the content usage record information of the EMD service centre 1 to JASRAC. The log data managing portion 15 sends fee information that indicates the content usage record of a user to the copyright managing portion 13 and the profit distribution portion 16. The profit distribution portion 16 computes the billing amount and paid amount for JASRAC, and sends this information to the accounting portion 20. The accounting portion 20 executes a settlement processing in communication with an external bank or the like not shown in the diagram. The copyright managing portion 13 sends the content usage record of a user to JASRAC.

[0087] The processing of an EMD system will be hereinafter described. FIG. 30 is a flowchart for describing the content distribution and reproduction processing of this system. In Step S11, the content provider managing portion 12 of the EMD service centre 1 sends a delivery key Kd to the content provider 2, and this is received by the content provider 2. The details of this processing will be described later with reference to the flowchart of FIG. 32. In Step S12, a user operates an device (for example, the receiver 51 of FIG. 10) of the user home network 5, and the device of the user home network 5 is registered in the user managing portion 18 of the EMD service centre 1. The details of this registration processing will be described later with reference to the flowchart of FIG. 36. In Step S13, the user managing portion 18 of the EMD service centre 1 performs a cross-authentication with the user home network 5 as shown in FIGS. 33 to 35, and then sends a delivery key Kd to the device of

the user home network 5. This key is received by the user home network 5. The details of this processing will be described later with reference to the flowchart of FIG. 44.

[0088] In Step S14, the secure container producing portion 38 of the content provider 2 sends a content provider secure container to the service provider 3. The details of this send processing will be described later with reference to FIG. 46. In Step S15, the secure container producing portion 44 of the service provider 3 sends the service provider secure container to the user home network 5 via the network 4 in response to a request from the user home network 5. The details of this send processing will be described later with reference to the flowchart of FIG. 48. In Step S16, a fee module 72 of the user home network 5 executes a fee processing. The details of this fee processing will be described later with reference to FIG. 50. In Step S17, the user reproduces the content using the device of the user home network 5. The details of this reproduction processing will be described later with reference to the flowchart of FIG. 51.

[0089] On the other hand, the flowchart of FIG. 31 illustrates the processing performed by the content provider 2 for encrypting and sending a usage policy. In Step S21, the content provider managing portion 12 of the EMD service centre 1 sends a delivery key Kd to the content provider 2. In Step S22, the service provider managing portion 11 of the EMD service centre 1 sends the delivery key Kd to the service provider 3. The subsequent processing of Steps S23 to S28 is the same as the processing performed in Steps S12 to S17 of FIG. 30 and, accordingly, a description thereof has been omitted.

[0090] FIG. 32 is a flowchart for describing the details of a processing correspondent to Step S11 of FIG. 30 and Step S21 of FIG. 31 by which the EMD service centre 1 sends a delivery key Kd to the content

provider 2, and this is received by the content provider 2. In Step S31, the cross-authenticating portion 17 of the EMD service centre 1 performs a cross-authentication with the cross-authenticating portion 39 of the content provider 2. The details of this cross-authentication processing will be described later with reference to the flowchart of FIG. 33. When the content provider 2 is authenticated as being a legitimate provider as a result of this cross-authentication processing, in Step S32, the encrypting portion 34 and the encrypting portion 36 of the content provider 2 receives the delivery key Kd transmitted from the content provider managing portion 12 of the EMD service centre 1. In Step S33, the encrypting portion 34 of the content provider 2 stores the received delivery key Kd.

[0091] In this way, the content provider 2 receives the delivery key Kd from the EMD service centre 1. Similarly, in the example processing of the flowchart shown in FIG. 31, in addition to the content provider 2, the service provider 3 also receives a delivery key Kd from the EMD service centre 1 based on a processing identical to that described in FIG. 32.

[0092] A cross-authentication processing for confirming the absence of so-called "spoofing" in Step S31 of FIG. 32 will be hereinafter described using a case in which one common key is used (FIG. 33), a case in which two common keys are used (FIG. 34), and a case in which a public key cipher is employed (FIG. 35) as examples.

[0093] FIG. 33 is a flowchart for describing the cross-authentication operation between the cross-authenticating portion 39 of the content provider 2 and the cross-authenticating portion 17 of the EMD service centre 1 employing common-key DES cryptography with a single common key. In Step S41, the cross-authenticating portion 39 of the content provider 2 generates a 64-bit random number R1 (this may also be generated by the random number generating portion 35). In Step S42, the cross-authenticating portion 39 of the

content provider 2 employs a DES to encrypt the random number R1 with a prestored common key Kc (this encryption may also be performed by the encrypting portion 36). In Step S43, the cross-authenticating portion 39 of the content provider 2 sends the encrypted random number R1 to the cross-authenticating portion 17 of the EMD service centre 1.

[0094] In Step S44, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the received random number R1 with the prestored common key Kc. In Step S45, the cross-authenticating portion 17 of the EMD service centre 1 generates a 32-bit random number R2. In Step S46, the cross-authenticating portion 17 of the EMD service centre 1 replaces the low-order 32 bits of the decrypted 64-bit random number R1 with the random number R2 to generate a concatenation $R1_H \| R2$ Notably, Ri_H denotes the high order bits of Ri, and $A \| B$ is a concatenation of A and B ((n+m) bits obtained by coupling the m-bits of B with the low-order n bits of A). In Step S47, the cross-authenticating portion 17 of the EMD service centre 1 employs DES to encrypt $R1_H \| R2$ with a common key Kc. In Step S48, the cross-authenticating portion 17 of the EMD service centre 1 sends the encrypted $R1_H \| R2$ to the content provider 2.

[0095] In Step S49, the cross-authenticating portion 39 of the content provider 2 decrypts the received $R1_H \| R2$ with the common key Kc. In Step S50, the cross-authenticating portion 39 of the content provider 2 checks the high-order 32 bits of the decrypted $R1_H \| R2$ against the high-order 32 bits $R1_H$ and if they match the random number R1 generated in Step S41 this certifies that the EMD service centre 1 is a legitimate centre. If the generated $R1_H$ and received $R1_H$ do not match, the processing ends. If the two match, in Step S51 the cross-authenticating portion 39 of the content provider 2 generates a 32-bit random number R3. In Step S52, the cross-authenticating portion 39 of the content provider 2 sets the received and decrypted 32 bit random number R2 in the high-order position, sets the generated

random number R3 in the low-order position thereof, and produces a concatenation R2‖R3. In Step S53, the cross-authenticating portion 39 of the content provider 2 employs DES to encrypt the concatenation R2R3 with the common key Kc. In Step S54, the cross-authenticating portion 39 of the content provider 2 sends the encrypted concatenation R2‖R3 to the cross-authenticating portion 17 of the EMD service centre 1.

[0096] In Step S55, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the received concatenation R2‖R3 with the common key Kc. In Step S56, the cross-authenticating portion 17 of the EMD service centre 1 checks the high-order 32 bits of the decrypted concatenation R2‖R3 against the random number R2 and, if they match, this certifies that the content provider 2 is legitimate and, if they do not, the provider is deemed to be illegitimate and the processing ends.

[0097] FIG. 34 is a flowchart for describing the cross-authentication operation between the cross-authenticating portion 39 of the content provider 2 and the cross-authenticating portion 17 of the EMD service centre 1 employing common-key DES cryptography using two common keys Kc1 and Kc2. In Step S61, the cross-authenticating portion 39 of the content provider 2 generates a 64-bit random number R1. In Step S62, the cross-authenticating portion 39 of the content provider 2 employs DES to encrypt the random number R1 with a prestored common key Kc1. In Step S63, the cross-authenticating portion 39 of the content provider 2 sends the encrypted random number R1 to the EMD service centre 1.

[0098] In Step S64, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the received random number R1 with a prestored common key Kc1. In Step S65, the cross-authenticating portion 17 of the EMD service centre 1 encrypts the random number R1 with a prestored common key Kc2. In Step S66, the cross-authenticating portion 17 of the EMD service centre 1

generates a 64-bit random number R2. In Step S67, the cross-authenticating portion 17 of the EMD service centre 1 encrypts the random number R2 with the common key Kc2. In Step S68, the cross-authenticating portion 17 of the EMD service centre 1 sends the encrypted random numbers R1 and R2 to the cross-authenticating portion 39 of the content provider 2.

[0099] In Step S69, the cross-authenticating portion 39 of the content provider 2 decrypts the received random numbers R1 and R2 with the prestored common key Kc2. In Step S70, the cross-authenticating portion 39 of the content provider 2 checks the decrypted random number R1 against the random number R1 generated in Step S61 (the random number R1 prior to encryption) and, if they match, this certifies that the EMD service centre 1 is legitimate, while if they do not match, the EMD service centre 1 is deemed to be illegitimate and the processing ends. In Step S71, the cross-authenticating portion 39 of the content provider 2 encrypts the decrypted random number R2 with the common key Kc1. In Step S72, the cross-authenticating portion 39 of the content provider 2 sends the encrypted random number R2 to the EMD service centre 1.

[0100] In Step S73, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the received random number R2 with the common key Kc1. In Step S74, the cross-authenticating portion 17 of the EMD service centre 1 checks the decrypted random number R2 against the random number R2 generated in Step S66 (the random number R2 prior to encryption) and, if they match, this certifies that the content provider 2 is a legitimate provider, while if they do not, the content provider 2 is deemed to be illegitimate and the processing ends.

[0101] FIG. 35 is a flowchart for describing the cross-authentication operation between the cross-authenticating portion 39 of the content provider 2 and the cross-authenticating portion 17 of the EMD service centre 1 employing a 160-bit length elliptic curve cipher as the public-key cryptography cipher. In Step

S81, the cross-authenticating portion 39 of the content provider 2 generates a 64-bit random number R1. In Step S82, the cross-authenticating portion 39 of the content provider 2 sends an authentication certificate (acquired in advance from a certifying agency) containing its own public key Kpcp along with the random number R1 to the cross-authenticating portion 17 of the EMD service centre 1.

[0102] In Step S83, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the signature of the received authentication certificate (encrypted with a secret key Ksca of the certifying agency) with the secret key Ksca of the certifying agency acquired in advance, extracts the hash value of a public key Kpcp of the content provider 2 and the name of the content provider 2, and extracts the public key Kpcp and name of the content provider 2 stored without alteration as plain text in the authentication certificate. If the authentication certificate is a legitimate authentication certificate issued by the certifying agency, this signature of the authentication certificate is able to be decrypted, and the thus-obtained hash value of the public key Kpcp and the name of the content provider 2 will match the hash value obtained by the application of a hash function to the public key Kpcp of the content provider 2 and the name of the content provider 2 contained as plain text in the authentication certificate. This certifies that the public key Kpcp is legitimate and has not been falsified. If the signature cannot be decrypted, or if it can but the hash values do not match, the public key or the provider is deemed to be illegitimate. In this case, the processing ends.

[0103] When a legitimate authentication result is obtained, the cross-authenticating portion 17 of the EMD service centre 1 generates a 64-bit random number R2 in Step S84. In Step S85, the cross-authenticating portion 17 of the EMD service centre 1 generates a concatenation R1‖R2 of the random numbers R1 and R2. In

Step S86, the cross-authenticating portion 17 of the EMD service centre 1 encrypts the concatenation R1‖R2 with its own secret key Ksesc. In Step S87, the cross-authenticating portion 17 of the EMD service centre 1 encrypts the concatenation R1‖R2 with the public key Kpcp of the content provider 2 obtained in Step S83. In Step S88, the cross-authenticating portion 17 of the EMD service centre 1 sends the concatenation R1‖R2 encrypted with the secret key Ksesc, the concatenation R1‖R2 encrypted by the public key Kpcp, and an authentication certificate (acquired in advance from the certifying agency) containing its own public key Kpesc to the cross-authenticating portion 39 of the content provider 2.

[0104] In Step S89, the cross-authenticating portion 39 of the content provider 2 decrypts the signature of the received authentication certificate with the secret key Kpca of the certifying agency acquired in advance and, if legitimate, extracts the public key Kpesc from the authentication certificate. This processing is the same as the processing performed in Step S83 and, accordingly, a description thereof has been omitted. In Step S90, the cross-authenticating portion 39 of the content provider 2 decrypts the concatenation R1‖R2 encrypted with the secret key Ksesc with the public key Kpesc acquired in Step S89. In Step S91, the cross-authenticating portion 39 of the content provider 2 decrypts the concatenation R1‖R2 encrypted with its own public key Kpcp with its own secret key Kscp. In Step S92, the cross-authenticating portion 39 of the content provider 2 compares the concatenation R1‖R2 decrypted in Step S90 with the concatenation R1‖R2 decrypted in Step S91 and, if they match, this certifies that the EMD service centre 1 is legitimate while, if they do not match, the EMD service centre 1 is deemed to be illegitimate and the processing ends.

[0105] When a legitimate authentication result is obtained, the cross-authenticating portion 39 of the content provider 2 generates a 64-bit random number R3

in Step S93. In Step S94, the cross-authenticating portion 39 of the content provider 2 generates a concatenation R2‖R3 of the random number R2 obtained in Step S90 and the random number R3 generated in Step S93. In Step S95, the cross-authenticating portion 39 of the content provider 2 encrypts the concatenation R2‖R3 with the public key Kpesc obtained in Step S89. In Step S96, the cross-authenticating portion 39 of the content provider 2 sends the encrypted concatenation R2‖R3 to the cross-authenticating portion 17 of the EMD service centre 1.

[0106] In Step S97, the cross-authenticating portion 17 of the EMD service centre 1 decrypts the encrypted concatenation R2‖R3 with its own secret key Ksesc. In Step S98, the cross-authenticating portion 17 of the EMD service centre 1 checks the decrypted random number R2 against the random number R2 generated in Step S84 (the random number R2 prior to encryption) and, if they match, it certifies that the content provider 2 is legitimate while, if they do not, the content provider 2 is deemed to be illegitimate and the processing ends.

[0107] As described above, the cross-authenticating portion 17 of the EMD service centre 1 and the cross-authenticating portion 39 of the content provider 2 perform cross-authentication. The random numbers used for cross-authentication are temporary keys Ktemp valid only for the processings subsequent to this cross-authentication.

[0108] FIG. 36 is a flowchart for describing an operation correspondent to Step S12 of FIG. 30 and Step S23 of FIG. 31 by which the receiver 51 is registered in the user managing portion 18 of the EMD service centre 1. In Step S101, the SAM 62 of the receiver 51 executes a processing in which, based on output from an IC card interface 64, it judges whether a backup IC card 55 is loaded in the receiver 51 and, where a backup IC card 55 is judged to be loaded therein (for example, where a receiver 51 is converted to a new receiver 51 and, in order for the data of the original

receiver 51 to be transferred to new receiver 51, the data of the original receiver 51 is backed up to the backup IC card 55), the procedure advances to Step S102 and the backup data stored in the IC card 55 is read. The details of this processing will be described later with reference to the flowchart of FIG. 41. While this backup data must of course be stored in the IC card 55 in advance in order to execute this read processing, this processing will be described later with reference to FIG. 39.

[0109] If the judgment in Step S101 is that the backup IC card 55 has not been loaded, the procedure skips Step S102 and advances to Step S103. In Step S103, the cross-authentication module 71 of the SAM 62 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1, and the SAM 62 sends an authentication certificate to the user managing portion 18 of the EMD service centre 1. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S103, the authentication certificate transmitted to the user managing portion 18 of the EMD service centre 1 by the SAM 62 contains the data shown in FIG. 37. While the authentication certificate transmitted by the SAM 62 has a configuration essentially the same as the authentication certificate of the content provider 2 shown in FIG. 14, it contains additional data that indicates whether or not it is subordinate to another SAM. In Step S104, the SAM 62 sends information and so on of a settlement agency such as the user's bank encrypted with the temporary key Ktemp to the user managing portion 18 of the EMD service centre 1 via the communicating portion 61.

[0110] In Step S105, the user managing portion 18 of the EMD service centre 1 searches the user registration database shown in FIG. 7 on the basis of the received ID of the SAM 62. In Step S106, the user managing portion 18 of the EMD service centre 1 judges whether

or not the SAM 62 of the received ID can be registered and, where it is judged that the SAM 62 of the received ID can be registered, the procedure advances to Step S107 and the SAM 62 of the received ID is judged as being newly registered. When the SAM 62 of the received ID is judged as not being newly registered in Step S107, the procedure advances to Step S108.

[0111] In Step S108, the user managing portion 18 of the EMD service centre 1 executes the new registration, and searches the user registration database on the basis of the received ID and produces a registration list. This registration list is, for example, of a structure as shown in FIG. 38, and is configured from, correspondent to the ID of the SAM of the device, a registration refusal flag indicating whether or not registration has been refused by the user managing portion 18 of the EMD service centre 1, a status flag indicating the usage conditions of the content key Kco for a subordinate device, a condition flag indicating whether or not the device is a subordinate device, and a signature obtained by encoding a hash value generated by application of a hash function to the registration refusal flag, status flag and condition flag with a secret key Ksesc of the EMD service centre 1.

[0112] The ID of the SAM of the device expresses an ID constituted from 64 bits peculiar to the device (in FIG. 38 expressed as a hexdecimal number). A "1" of the registration refusal flag indicates that the user managing portion 18 of the EMD service centre 111 has registered the device of the corresponding ID, and an "0" of the registration denial flag indicates that the user managing portion 18 of the EMD service centre 1 has refused the registration of the device of the corresponding ID.

[0113] An MSB (Most Significant Bit) "1" of the status flag indicates that a content key can be received from a "parent" device (for example receiver 51) to which a "child" device (for example recorder 53) of a correspondent ID is subordinate, and an MSB "0" of the

status flag indicates that a content key Kco cannot be received from the "parent" device to which the "child" device of the correspondent ID is subordinate. A 2nd bit "1" from the highest order of the status flag indicates that a content key Kco encrypted by a saved key Ksave of the "parent" device is able to be received from the "parent" device to which a "child" device of the correspondent ID is subordinate. A 3rd bit "1" from the highest order of the status flag indicates that a content key Kco encrypted with a delivery key Kd is able to be received from a "parent" device to which a "child" device of a correspondent ID is subordinate. An LSB (Least Significant Bit) "1" of the status flag indicates that a subordinate "parent" device has purchased a content key Kco encrypted with a delivery key Kd, and that the content key Kco encrypted with the temporary key Ktemp has been transferred to a "child" device of the correspondent ID.

[0114] The "0" of the condition flag indicates that a device of the corresponding ID (that is to say, for example, a "parent" device such as the receiver 51) is able to directly communicate with the user managing portion 18 of the EMD service centre 1, and the "1" of the condition flag indicates that a device of the correspondent ID (that is to say, a "child" device such as a recorder 53) is not able to directly communicate with the user managing portion 18 of the EMD service centre 1. When the condition flag is "0", the status flag is always set to "0000".

[0115] In Step S109, the user managing portion 18 of the EMD service centre 1 sends the delivery key Kd supplied from the key server 14 encrypted with the temporary key Ktemp supplied from the cross-authenticating portion 17 to the SAM 62 of the receiver 51. In Step S110, the SAM 62 of the receiver 51 encrypts the delivery key Kd with the temporary key Ktemp and stores the result in the storage module 73.

[0116] In Step S111, the user managing portion 18 of the EMD service centre 1 sends the registration list

encrypted with the temporary key Ktemp to the SAM 62 of the receiver 51. In Step S112, the SAM 62 of the receiver 51 encrypts the received registration list with the temporary key Ktemp, and stores the result in the storage module 73 which ends the processing.

[0117] In Step S107, if the SAM 62 of the received ID is judged as being newly registered, the procedure advances to Step S114, and the user managing portion 18 of the EMD service centre 1 then executes a new registration and produces a registration list, and the procedure then advances to Step S109.

[0118] If the SAM 62 of the received ID is judged in Step S106 as being unable to be registered, the procedure advances to Step S113 where the user managing portion 18 of the EMD service centre 1 produces a registration refusal registration list; and the procedure then advances to Step S111.

[0119] In this way, the receiver 51 is registered in the EMD service centre 1.

[0120] The details of the processing for storing predetermined data such as the delivery key Kd stored in the hitherto used storage module 73 of the receiver 51 in the IC card 55 will be hereinafter described with reference to the flowchart of FIG. 39. In Step S121, the cross-authentication module 71 of the SAM 62 performs a cross-authentication with a cross-authentication module 80 of the IC card 55. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S122, a random number generation unit 92 of the SAM 62 generates a random number employed as a backup key Kic. In Step S123, the encryption unit 93 of the SAM 62 encrypts the ID number of the SAM stored in the storage module 73, the save key Ksave, and the ID of the HDD 52 with the backup key Kic. In Step S124, the encryption unit 93 of the SAM 62 encrypts the backup key Kic with a public key Kpesc of the EMD service centre 1 (in the authentication processing with the EMD

service centre 1 (Step S89 of FIG. 35), the SAM 62 acquires the public key Kpesc of the EMD service centre 1). In Step S125, the SAM 62 of the receiver 51 sends the ID number of the encrypted SAM, the save key Ksave, the ID of the HDD 52 and the encrypted backup key Kic to the IC card 55 via the IC card interface 64 for storage in the storage module 81.

[0121] As described above, the ID number of the SAM stored in the storage module 73 of the SAM 62, the save key Ksave and the ID of the HDD 52 are encrypted employing the backup key Kic, and are stored in the cross-authentication module 81 of the IC card 55 together with the backup key Kic encrypted employing the public key Kpesc of the EMD service centre 1.

[0122] The details of another example of the processing by which predetermined data such as the delivery key Kd stored in a hitherto used storage module 73 of a receiver 51 in a IC card 55 will be described with reference to the flowchart of FIG. 40. In Step S131, the cross-authentication module 71 of the SAM 62 performs a cross-authentication with the cross-authentication module 80 of the IC card 55. In Step S132, the encryption unit 93 of the SAM 62 employs the public key Kpesc of the EMD service centre 1 to encrypt the ID number of the SAM stored in the storage module 73, the save key Ksave and the ID of the HDD 52. In Step S133, the SAM 62 of the receiver 51 sends the encrypted ID number of the SAM, the save key Ksave and the ID of the HDD 52 to the IC card 55 via the IC card interface 64 for storage in the cross-authentication module 81.

[0123] Based on the processing of FIG. 40, the ID number of the SAM, the save key Ksave and the ID of the HDD 52 encrypted employing the public key Kpesc of the EMD service centre 1 are stored in the cross-authentication module 81 of the IC card 55 by a simpler processing than the processing described in FIG. 39.

[0124] In this way, data backed up on the IC card 55, is loaded into a new receiver 51 by the processing of

Step S102 of FIG. 36. FIG. 41 is a flowchart for describing the processing for reading the data backed up by the processing of FIG. 39. In Step S141, the cross-authentication module 71 of the SAM 62 of the new receiver 51 performs cross-authentication with the cross-authentication module 80 of the IC card 55. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted.

[0125] In Step S142, the SAM 62 reads, via the IC card interface 64, the data (backup data of the ID number of the SAM, the save key Ksave and ID of the HDD 52) of the storage module 73 of the previous receiver 51 encrypted with the backup key Kic and the backup key Kic encrypted with the public key Kpesc of the EMD service centre 1 stored in the cross-authentication module 81. In Step S143, the cross-authentication module 71 of the SAM 62 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1 via the communicating portion 61. This cross-authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S144, the SAM 62 sends the data of the storage module 73 encrypted with the backup key Kic and backup data Kic encrypted with the public key Kpesc of the EMD service centre 1 to the user managing portion 18 of the EMD service centre 1.

[0126] In Step S145, the user managing portion 18 of the EMD service centre 1 decrypts the received backup key Kic with its own secret key Ksesc. In Step S146, the user managing portion 18 of the EMD service centre 1 decrypts the received backup data with the backup key Kic. In Step S147, the user managing portion 18 of the EMD service centre 1 re-encrypts the decrypted backup data with the temporary key Ktemp supplied from the cross-authenticating portion 17. In Step S148, the user managing portion 18 of the EMD service centre 1 sends

the backup data encrypted with the temporary key Ktemp to the communicating portion 61 of the receiver 51.

[0127] In Step S149, the communicating portion 61 sends the data received from the user managing portion 18 of the EMD service centre 1 to the SAM 62 and, after decrypting this data, the SAM 62 stores the result thereof in the storage module 73. In Step S150, the user managing portion 18 of the EMD service centre 1 sets the data of the user registration database (FIG. 7) correspondent to the ID of the SAM 62 of the previous device for which data is stored in the IC card 55 to "unregistered", and the processing ends.

[0128] In this way, the new receiver 51 reads the backup data of the IC card 55.

[0129] The processing for reading the data backed up by the processing of FIG. 40 will be described with reference to FIG. 42. In Step S161, the cross-authentication module 71 of the SAM 62 of the receiver 51 performs a cross-authentication with the cross-authentication module 80 of the IC card 55. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S162, the SAM 62, via the IC card interface 64, reads the data (backup data of the ID number of the SAM, the save key Ksave and the ID of the HDD 52) of the storage module 73 of a previous receiver 51 encrypted with the public key Kpesc of the EMD service centre 1.

[0130] In Step S163, the cross-authentication module 71 of the SAM 62 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1 via the communicating portion 61. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S164, the SAM 62 sends the data of the storage module 73 encrypted with the public key Kpesc of the EMD service centre 1 via the communicating portion 61

to the user managing portion 18 of the EMD service centre 1.

[0131] In Step S165, the user managing portion 18 of the EMD service centre 1 decrypts the received data of the storage module 73 with its own secret key Ksesc. In Step S166, the user managing portion 18 of the EMD service centre 1 re-encrypts the decrypted backup data with the temporary key Ktemp supplied from the cross-authenticating portion 17. In Step S167, the user managing portion 18 of the EMD service centre 1 sends the backup data encrypted with the temporary key Ktemp to the communicating portion 61 of the receiver 51.

[0132] In Step S168, the communicating portion 61 of the receiver 51 sends the data received from the user managing portion 18 of the EMD service centre 1 to the SAM 62 and, after decrypting this data, the SAM 62 stores the result thereof in the storage module 73. In Step S169, the user managing portion 18 of the EMD service centre 1 sets the data of the user registration database (FIG. 7) correspondent to the ID of the SAM 62 of the previous device for which data is stored in the IC card 55 as "unregistered".

[0133] In this way, for backup in which the processing shown in FIG. 40 is employed, the receiver 51 reads the backup data of the IC card 55 by the processing of FIG. 42.

[0134] While the receiver 51 executes the processing of the flowchart of FIG. 36 when performing its own registration (executes a processing correspondent to Step S12 of FIG. 30), it executes the processing of the flowchart of FIG. 43 when registering the recorder 53 subordinate to the receiver 51 in the EMD service centre 1. In Step S181, the SAM 62 of the receiver 51 writes the ID of the recorder 53 in the registration list stored in the storage module 73. In Step S182, the cross-authentication module 71 of the receiver 51 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1. This authentication processing is the same as the

processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted.

[0135] In Step S183, the user managing portion 18 of the EMD service centre 1 searches the user registration database on the basis of the ID of the receiver 51 (ID of the SAM 62 contained in the authentication certificate of the SAM 62 shown in FIG. 37) and judges whether or not the receiver 51 is unregistered and, if the receiver 51 is judged to be unregistered, the procedure advances to Step S184 where the SAM 62 of the receiver 51, for the user managing portion 18 of the EMD service centre 1, encrypts the version of the delivery key Kd stored in the storage module 73, the fee information (stored by the later-described processing of Step S337 of the flowchart of FIG. 50), the registration list and the usage policy recorded in the HDD 52 with the delivery key Kd and sends the version of the delivery key Kd stored in the storage module 73, the fee information, the registration list and the usage policy recorded in the HDD 52 to the user managing portion 18 of the EMD service centre 1 via the communicating portion 61. In Step S185, the user managing portion 18 of the EMD service centre 1, after decrypting the received data, executes a fee information processing, and updates sections of data such as the registration refusal flag and status flag and so on pertaining to the recorder 53 of the registration list received from the receiver 51 described with reference to FIG. 38, and appends a signature in accordance with this data correspondent to the receiver 51.

[0136] In Step S186, the user managing portion 18 of the EMD service centre 1 judges whether or not the version of the delivery key Kd possessed by the receiver 51 has been updated and, where it judges that the version of the delivery key Kd possessed by the receiver 51 has been updated, the procedure advances to Step S187 where the updated registration list and a fee

information receipt message encrypted with the delivery key Kd are transmitted to the receiver 51 and, subsequent to receiving and decrypting this updated registration list and fee information receipt message, the receiver 51 stores this information. In Step S188, the receiver 51 deletes the fee information stored in the storage module 73 and updates the registration list to the registration list received in Step S187 from the user managing portion 18 of the EMD service centre 1, after which the procedure advances to Step S191.

[0137] Where it is judged in Step S186 that the version of the delivery key Kd possessed by the receiver 51 has not been updated, the procedure advances to Step S189 where the user managing portion 18 of the EMD service centre 1 sends the updated version of the delivery key Kd, the updated registration list and the fee information receipt message encrypted with a delivery key Kd to the receiver 51 and, after receiving and decrypting the updated version of the delivery key Kd, the updated registration list and the fee information receipt message, the receiver 51 stores this information. In Step S190, the receiver 51 deletes the fee information stored in the storage module 73, updates the registration list to the list received in Step S189 from the user managing portion 18 of the EMD service centre 1 and updates the delivery key Kd to the updated version, after which the procedure advances to Step S191.

[0138] In Step S191, the SAM 62 of the receiver 51 references the updated registration list and judges whether or not the recorder 53 is unregistered and, where the recorder 53 is judged to be unregistered, the procedure advances to Step S192 where cross-authentication between the receiver 51 and the recorder 53 is performed and a temporary key Ktemp is shared. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S193, a registration completion

message and a delivery key Kd encrypted with the temporary key Kd is transmitted to the recorder 53, and the recorder 53 receives and decrypts the registration completion message and delivery key Kd. In Step S194, the recorder 53 updates the delivery key Kd, and then the processing ends.

[0139] Where it is judged in Step S183 that the receiver 51 is unregistered and it is judged in Step S191 that the recorder 53 is unregistered, the processing ends.

[0140] As described above, the recorder 53 subordinate to the receiver 51 is registered in the EMD service centre 1 via the receiver 51.

[0141] FIG. 44 is a flowchart for describing the details of the processing by which, in Step S13 of FIG. 30, the receiver 51 receives the delivery key Kd transmitted to the receiver 51 by the EMD service centre 1. In Step S201, the cross-authentication module 71 of the receiver 51 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S202, the SAM 62 of the receiver 51 sends an authentication certificate to the user managing portion 18 of the EMD service centre 1 via the communicating portion 61, and the user managing portion 18 of the EMD service centre 1 receives this authentication certificate. Steps 203 to 210 describe a processing the same as the processing of Steps S183 to 190 of FIG. 43 and, accordingly, a description thereof has been omitted.

[0142] In this way, the receiver 51 receives the delivery key Kd from the user managing portion 18 of the EMD service centre 1, and sends the fee information of the receiver 51 to the user managing portion 18 of the EMD service centre 1.

[0143] The processing for receipt of the delivery key Kd of the recorder 53 subordinate to the receiver 51

(where the status flag of FIG. 38 is a value that permits receipt of the delivery key Kd of the recorder 53) will be hereinafter described with reference to FIG. 45. In Step S221, cross-authentication is performed between the cross-authentication module 71 of the receiver 51 and a cross-authentication module not shown in the diagram of the recorder 53. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted.

[0144] In Step S222, the receiver 51 judges whether or not the data of the recorder 53 is listed in the registration list stored in the storage module 73 of the receiver 51 and, where the data of the recorder 53 is judged as being listed in the registration list stored in the storage module 73 of the receiver 51, the procedure advances to Step S223 where, on the basis of the registration list stored in the storage module 73 of the receiver 51, the recorder 53 is judged as being unregistered. Where the recorder 53 is judged as unregistered in Step S223, the procedure advances to Step S224, and the SAM 66 of the recorder 53 encrypts and sends the version of the delivery key Kd stored in an internal module (received from the receiver 51 in the later-described Step 235 of FIG. 45) and fee information (stored by a processing equivalent to a later-described Step S337 of a processing correspondent to FIG. 50) with a temporary key Ktemp to the SAM 62 of the receiver 51, and the SAM 62 of the receiver 51 receives and decrypts the version of the delivery key Kd and the fee information.

[0145] In Step S225, the cross-authentication module 71 of the receiver 51 performs cross-authentication with the cross-authenticating portion 17 of the EMD service centre 1 via the communicating portion 61. This authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S226, the user managing portion 18 of the EMD

service centre 1 searches the user registration database on the basis of the ID of the receiver 51 and judges whether or not the receiver 51 is unregistered and, where the receiver 51 is judged as unregistered, the procedure advances to Step S227 where the SAM 62 of the receiver 51, via the communicating portion 61, sends the version of the delivery key Kd, the fee information, the registration list, the usage policy recorded in the HDD 52 and the fee information of the recorder 53 stored in the storage module 73 and encrypted with the delivery key Kd to the user managing portion 18 of the EMD service centre 1. In Step S228, the user managing portion 18 of the EMD service centre 1, after decrypting the received data, performs a fee information processing, updates the data sections such as the registration refusal flag, status flag pertaining to the recorder 53 received from the receiver 51 described by FIG. 38, and appends a signature in accordance with data correspondent to the receiver 51.

[0146] The processing of each of Steps 229 to 234 is the same as the processing of Steps 186 to 191 and, accordingly, a description thereof has been omitted.

[0147] In Step S234, the SAM 62 of the receiver 51 references the updated registration list and judges whether or not the recorder 53 is unregistered and, where the recorder 53 is judged as unregistered, the procedure advances to Step S235 where the fee information receipt message and delivery key Kd encrypted with the delivery key Kd are transmitted to the recorder 53, and the recorder 53 receives and decrypts this fee information receipt message and delivery key Kd. In Step S236, the SAM 66 of the recorder 53 deletes the fee information stored in the internal storage module, and updates the delivery key Kd to a revised version.

[0148] Where it is judged in Step S222 that the data of the recorder 53 is not listed in the registration list stored in the storage module 73 of the receiver 51, the

procedure advances to Step S237 where the registration processing of the recorder 53 described in FIG. 43 is executed, after which the procedure advances to Step S224.

[0149] Where the recorder 53 is judged as unregistered in Step S223, the receiver 51 is judged as unregistered in Step S226, or the recorder 53 is judged as unregistered in Step S234, the processing ends.

[0150] As described above, the recorder 53 subordinate to the receiver 51 receives the delivery key Kd via the receiver 51.

[0151] The processing by which the content provider 2 sends the content provider secure container to the content provider 2 correspondent to Step S14 of FIG. 30 will be hereinafter described with reference to the flowchart of FIG. 46. In Step S251, the watermarking portion 32 of the content provider 2 inserts a predetermined watermark denoting the content provider 2 into the content read from the content server 31, and supplies this content to the compressing portion 33. In Step S252, the compressing portion 33 of the content provider 2 compresses the content into which a watermark has been inserted by a predetermined method such as ATRAC2, and supplies this to the encrypting portion 34. In Step S253, the random number generating portion 35 generates a random number to be employed as a content key Kco and supplies this to the encrypting portion 34. In Step S254, the encrypting portion 34 of the content provider 2 encrypts the compressed content in which the watermark has been inserted by a predetermined method such as DES using the content key Kco generated by the random number generating portion 35.

[0152] In Step S255, the encrypting portion 36 encrypts the content key Kco by a predetermined method such as DES with the delivery key Kd supplied by the EMD service centre 1 by the processing of Step S11 of FIG. 30. In Step S256, the secure container producing portion 38 of the content provider 2 computes a hash

value by applying a hash function to the encrypted content, the encrypted content key Kco and the usage policy supplied from policy storing portion 37, and encrypts this with its own secret key Ksesc to produce the signature shown in FIG. 13. In Step S257, the secure container producing portion 38 of the content provider 2 produces the content provider secure container shown in FIG. 13 which contains the encrypted content, the encrypted content key Kco, the usage policy supplied from policy storing portion 37 and the signature generated in Step S256.

[0153] In Step S258, the cross-authenticating portion 39 of the content provider 2 performs cross-authentication with the cross-authenticating portion 45 of the service provider 3. This cross-authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S259, the secure container producing portion 38 of the content provider 2 sends this content provider secure container with an authentication certificate issued in advance by a certifying agency appended thereto to the service provider 3, after which the processing ends.

[0154] As described above, the content provider 2 sends the content provider secure container to the service provider 3.

[0155] The details of another processing by which the content provider 2 sends a service provider secure container to the service provider 3 for an example based on a content Key Kco being encrypted together with a usage policy using a delivery key Kd will be described with reference to FIG. 47. The processing of Steps S271 to S274 is the same as the processing of Steps S251 to S254 of FIG. 46 and, accordingly, a description thereof has been omitted. In Step S275, the encrypting portion 36 of the EMD service centre 1 uses a predetermined method such as DES to encrypt the content key Kco and usage policy supplied from the policy storing portion 37 employing the delivery key Kd

supplied from the EMD service centre 1 by the processing of Step S21 of FIG. 31.

[0156] In Step S276, the secure container producing portion 38 of the EMD service centre 1 computes a hash value by applying a hash function to the encrypted content, the encrypted content key Kco, and the encrypted usage policy, and encrypts this with its own secret key Kscp to produce the signature shown in FIG. 25. In Step S277, the secure container producing portion 38 of the EMD service centre 1 produces the content provider secure container shown in FIG. 25 which contains the encrypted content, the encrypted content key Kco, the encrypted usage policy, and the signature. The processing of Steps S278 and 279 is the same as the processing of Steps S258 and S259 of FIG. 46 and, accordingly, a description thereof has been omitted.

[0157] In this way, the EMD service centre 1 sends the content provider 2 secure container containing an encrypted usage policy to the service provider 3.

[0158] The details of the processing correspondent to Step S15 of FIG. 30 by which the EMD service centre 1 sends a service provider secure container to the recorder 53 will be hereinafter described with reference to the flowchart of FIG. 48. In Step S291, the pricing portion 42 of the service provider 3 verifies the signature contained in the authentication certificate attached to the content provider secure container transmitted from the secure container producing portion 38 of the content provider 2 and, where the authentication certificate has not been falsified, extracts the public key Kpcp of the content provider 2 therefrom. The verification of the signature of the authentication certificate is the same as in the processing of Step S83 of FIG. 35 and, accordingly, a description thereof has been omitted.

[0159] In Step S292, the pricing portion 42 of the service provider 3 decrypts the signature of the content provider secure container transmitted from the

secure container producing portion 38 of the content provider 2 with the public key Kpcp of the content provider 2, verifies that the obtained hash value matches the hash value obtained by applying a hash function to the encrypted content, the encrypted content key Kco and the usage policy to verify that the content provider secure container has not been falsified and, if falsification is detected, the processing ends.

[0160] Where there is no falsification of the content provider secure container detected in Step S293, the pricing portion 42 of the service provider 3 extracts the usage policy from the content provider secure container. In Step S294, the pricing portion 42 of the service provider 3 produces the pricing information described in FIG. 17 on the basis of the usage policy. In Step S295, the secure container producing portion 44 of the service provider 3 produces the service provider secure container shown in FIG. 15 which contains the encrypted content, the encrypted content key Kco, the usage policy, the pricing information, and a signature of a value obtained by encrypting a hash value obtained by applying a hash function to the encrypted content, the encrypted content key Kco, the usage policy and the pricing information with its own secret key Kssp.

[0161] In Step S296, the cross-authenticating portion 45 of the service provider 3 performs cross-authentication with the cross-authentication module 71 of the receiver 51. This cross-authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. In Step S297, the secure container producing portion 44 of the service provider 3 sends the service provider secure container 4 to which the authentication certificate has been attached to the communicating portion 61 of the receiver 51.

[0162] In this way, the service provider 3 sends a service provider secure container to the receiver 51.

[0163] The details of the processing by which the service provider 3 sends a service provider secure container to the receiver 51 for an example based on the usage policy being encrypted with a delivery key Kd in the content provider 2 and usage control information being produced by the service provider 3 will be hereinafter described with reference to the flowchart of FIG. 49. The processing of Steps S311 and S312 is the same as the processing of Steps 291 and S292 of FIG. 48 and, accordingly, a description thereof has been omitted. In Step S313, the pricing portion 42 of the service provider 3 decrypts the encrypted usage policy contained in the content provider secure container. In Step S314, the pricing portion 42 of the service provider 3 produces the usage control information described in FIG. 23 on the basis of this usage policy. The processing of Steps S315 to S318 is the same as the processing of Steps 294 to S297 of FIG. 48 and, accordingly, a description thereof has been omitted.

[0164] In this way, the service provider 3 sends a service provider secure container containing an encrypted usage policy to the receiver 51.

[0165] The details of the fee processing of the receiver 51 correspondent to Step S16 of FIG. 30 executed subsequent to a legitimate service provider secure container being received will be hereinafter described with reference to the flowchart of FIG. 50. In Step S331, the encryption/decryption module 74 of the receiver 51 judges whether or not content key Kco can be decrypted with the delivery key Kd, and where the content key Kco is judged as not being able to be decrypted with the delivery key Kd, the receiver 51 executes a processing for receipt of the delivery key Kd described in FIG. 44 in Step S332, and the procedure then advances to Step S333. When the content key Kco is judged as being able to be decrypted by the delivery key Kd in Step S331, the procedure skips Step S332 and advances to Step S333. In Step S333, the decryption

unit 91 of the receiver 51 decrypts the content Kco with the delivery key Kd stored in the storage module 73 by the processing of Step S13 of FIG. 30.

[0166] In Step S334, the fee processing module 72 of the receiver 51 extracts the usage policy and pricing information contained in the service provider secure container, and generates the fee information and license conditions information described by FIG. 19 and FIG. 20. In Step S335, the fee processing module 72 of the receiver 51 judges whether or not a current calculated fee is higher than the calculated fee upper limit from the fee information computed in Step S334 and the fee information stored in the storage module 73 and, where the current calculated fee is judged to be higher than the upper limit, the procedure advances to Step S336 where the receiver 51 executes a processing for the receipt of a new delivery key Kd, described by FIG. 4, after which the procedure advances to Step S337. Where the current calculated fee is judged to be less than the calculated fee upper limit in Step S335, Step S336 is skipped and the procedure advances to Step S337.

[0167] In Step S337, the fee processing module 72 of the receiver 51 stores the fee information in the storage module 73. In Step S338, the fee processing module 72 of the receiver 51 records the license usage conditions information generated in Step S334 in the HDD 52. In Step S339, the SAM 62 of the receiver 51 records the usage policy extracted from the service provider secure container in the HDD 52.

[0168] In Step S340, the encryption/decryption module 74 of the receiver 51 applies a hash function to the license usage conditions information to compute a hash value. In Step S341, the storage module 73 of receiver 51 stores the hash value of the license usage conditions information. Where there is no save key Ksave stored in the storage module 73, the encryption unit 92 of the receiver 51 generates a random number in Step S342 which serves as the save key Ksave, and the

procedure then advances to Step S343. Where a save key Ksave is stored in the storage module 73, Step S342 is skipped and the procedure advances to Step S343.

[0169] In Step S343, the encryption unit 93 of the receiver 51 encrypts the content key Kco with the save key Ksave. In Step S344, the SAM 62 of the receiver 51 stores the encrypted content key Kco in the HDD 52. Where there is no save key Ksave stored in the storage module 73, the encryption/decryption module 74 stores a save key Ksave in the storage module 73 in Step S345, and the processing then ends. Where a save key Ksave is stored in the storage module 73, Step S345 is skipped and the processing ends.

[0170] As is described above, the receiver 51 stores the fee information in the storage module 73, decrypts the content key Kco with the delivery key Kd, re-encrypts the content key Kco with the save key Ksave, and stores this in the HDD 52. The save key Ksave is stored in the storage module 73.

[0171] The recorder 53, by a similar processing, stores the fee information in the storage module of the SAM 66, decrypts the content key Kco with the delivery key Kd, re-encrypts the content key Kco with a save key Ksave, and stores this in the HDD 52. The save key Ksave is stored in the storage module of the SAM 66.

[0172] The details of the processing correspondent to Step S17 of FIG. 30 by which the receiver 51 reproduces the content will be described with reference to FIG. 51. In Step S361, the encryption/decryption module 74 of the receiver 51 reads the license usage conditions information stored according to Step S338 of FIG. 50 and the content key Kco encrypted and stored according to Step S344 from the HDD 52. In Step S362, the encryption/decryption module 74 of the receiver 51 applies a hash function to the license usage conditions information to compute a hash value.

[0173] In Step 363, the encryption/decryption module 74 of the receiver 51 judges whether or not the hash value computed in Step S362 matches the hash value stored in

the storage module 73 according to S340 of FIG. 50, and where the hash value computed in Step S362 is judged as matching the hash value stored in the storage module 73, the procedure advances to Step S364 and the predetermined information contained in the license usage conditions information such as the usage frequency value is updated. In Step S365, the encryption/decryption module 74 of the receiver 51 applies a hash function to the updated license usage conditions to compute a hash value. In Step S366, the storage module 73 of the receiver 51 stores the hash value of the license usage conditions information computed in Step S365. In Step S367, the encryption/decryption module 74 of the receiver 51 records the updated license usage conditions information in the HDD 52.

[0174] In Step S368, the cross-authentication module 71 of the SAM 62 and the cross-authentication module 75 of the expanding portion 63 perform a cross-authentication, and the SAM 62 and expanding portion 63 store a temporary key Ktemp. This cross-authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. Random numbers R1, R2 or R3 employed in the cross-authentication serve as the temporary keys Ktemp. In Step S369, the decryption unit 91 of the encryption/decryption module 74 decrypts the content key Kco stored in the HDD 52 in Step S344 of FIG. 50 with the decrypted save key Ksave stored in the storage module 73. In Step S370, the encryption unit 93 of the encryption/decryption module 74 encrypts the decrypted content key Kco with the temporary key Ktemp. In Step S371, the SAM 62 sends the content key Kco encrypted with the temporary key Ktemp to the encrypting portion 363.

[0175] In Step S372, the decryption module 76 of the expanding portion 63 decrypts the content key Kco with the temporary key Ktemp. In Step S373, the SAM 62 reads the content recorded in the HDD 52 and sends this to

the expanding portion 63. In Step S374, the decryption module 77 of the expanding portion 63 decrypts the content with the content key Kco. In Step S375, an expansion module 78 of the expanding portion 63 expands the decrypted content using a predetermined method such as ATRAC. In Step S376, a watermarking module 79 of the expanding portion 63 inserts a predetermined watermark that identifies the receiver 51 into the expanded content. In Step S377, the receiver 51 outputs the reproduced content to a speaker or the like not shown in the diagram, and the processing ends.

[0176] Where it is judged in Step S363 that the hash value computed in Step S362 does not match the hash value stored in the storage module 73, in Step S378, the SAM 62 executes a predetermined error processing such as the display of an error message in a display device not shown in the diagram, and the processing ends.

[0177] In this way, the receiver 51 reproduces the content.

[0178] FIG. 52 is a flowchart for describing the processing by which, in the user home network 5 of the configuration shown in FIG. 11, a receiver 51 reproduces content in a decoder 56. The processing of Steps S391 to S397 is the same as the processing of Steps S361 to S367 of FIG. 51 and, accordingly, a description thereof has been omitted.

[0179] In Step S398, the cross-authentication module 71 of the SAM 62 and a cross-authentication module 101 of the decompressing portion 64 perform cross-authentication and share a temporary key Ktemp. This cross-authentication processing is the same as the processing described with reference to FIGS. 33 to 35 and, accordingly, a description thereof has been omitted. The random numbers R1, R2 and R3 employed for the cross-authentication serve as the temporary keys Ktemp. In Step S399, the decryption unit 91 of the encryption/decryption module 74 decrypts the content key Kco stored in the HDD 52 using the save key Ksave

stored in the storage module 73. In Step S400, the encryption unit 93 of the encryption/decryption module 74 encrypts the decrypted content key Kco using the temporary key Ktemp. In Step S401, the SAM 62 sends the encrypted content key Kco encrypted with the temporary key Ktemp to the decoder 56.

[0180] In Step S402, a decryption module 102 of the decoder 56 decrypts the content key Kco using the temporary key Ktemp. In Step S403, the SAM 62 reads the content recorded on the HDD 52 and sends this to the decoder 56. In Step S404, a decryption module 103 of the decoder 56 decrypts the content with the content key Kco. In Step S405, an expansion module 104 of the decoder 56 expands the decrypted content by a predetermined method such as ATRAC2. In Step S406, a watermarking module 105 of the decoder 56 inserts a watermark that identifies the decoder 56 into the expanded content. In Step S407, the decoder 56 outputs reproduced content to speakers or the like not shown in the diagram, and the processing ends.

[0181] The processing of Step S408 is the same as the processing of Step S378 of FIG. 51 and, accordingly, a description thereof has been omitted.

[0182] As is described above, for a user home network of the configuration shown in FIG. 11, content received by the receiver 51 reproduced by the decoder 56.

[0183] Notably, while in the description above music data is used as an example of content, content is not limited to music data alone, and moving image data, still image data, text data, or program data can also be employed. At this time, a compression method suitable for the content type such as MPEG (Moving Picture Experts Group) can be selected if the content is image data. A type of watermark of a format suitable for the content type is also used.

[0184] While the description given above uses a block cipher DES as the common-key cipher, FEAL proposed by NTT (Trademark), IDEA (International Data Encryption

Algorithm), or a stream cipher that encrypts a bit or several bits of data at a time can also be employed.

[0185] Furthermore, while the use of common-key cryptography for encrypting the content and the content key Kco is described above, public-key cryptography can also be used.

[0186] Notably, the term system used in this specification refers to an apparatus configured from a plurality of devices in its entirety.

[0187] In addition to recording media such as magnetic discs, CD-ROMs and solid state-memories, communications media such as satellites can also be used as the providing medium for providing the computer programs for executing the processings described above.

[0188] [Effect of the Invention] Based on the information processing apparatus according to Claim 1, the information processing method according to Claim 2, and the providing medium according to Claim 3, cross-authentication is performed, a temporary key is generated, a second key is stored, a first key is decrypted with the second key, the first key is encrypted with the temporary key, the first key is decrypted with the temporary key, and information is decrypted with the first key and, accordingly, the key used for encrypting the information cannot be read when the information is being decrypted.

[Brief Description of the Drawings]

[FIG. 1] is a diagram describing an EMD system;

[FIG. 2] is a block diagram illustrating a functional configuration of an EMD service centre 1;

[FIG. 3] is a diagram describing transmission of a delivery key Kd of the EMD service centre 1;

[FIG. 4] is another diagram describing transmission of a delivery key Kd of the EMD service centre 1;

[FIG. 5] is another diagram describing transmission of a delivery key Kd of the EMD service centre 1;

[FIG. 6] is another diagram is another diagram describing transmission of a delivery key Kd of the EMD service centre 1;

[FIG. 7] is a diagram describing a user registration database;

[FIG. 8] is a block diagram illustrating a functional configuration of a content provider 2;

[FIG. 9] is a block diagram illustrating a functional configuration of a service provider 3;

[FIG. 10] is a block diagram illustrating the configuration of a user home network 5;

[FIG. 11] is another block diagram illustrating a configuration of a user home network 5;

[FIG. 12] is a diagram describing content and information appended to the content;

[FIG. 13] is a diagram describing a content provider secure container;

[FIG. 14] is a diagram describing a certificate of the content provider 2;

[FIG. 15] is a diagram describing a service provider secure container;

[FIG. 16] is a diagram describing an authentication certificate of the service provider 3;

[FIG. 17] is a diagram illustrating a usage policy, pricing information and license usage conditions information;

[FIG. 18] is a diagram describing single copy and multiple copy;

[FIG. 19] is a diagram describing usage policy and pricing information;

[FIG. 20] is a diagram describing usage policy, pricing information and license usage conditions information;

[FIG. 21] is a diagram describing another configuration of content and information appended to the content;

[FIG. 22] is a diagram describing a service provider secure container;

[FIG. 23] is a diagram describing usage policy, usage control information, pricing information and license usage conditions information;

[FIG. 24] is a diagram describing another configuration of content and information appended to the content;

[FIG. 25] is a diagram describing a content provider secure container;

[FIG. 26] is a diagram describing a service provider secure container;

[FIG. 27] is a diagram describing an operation for receipt of fee information of the EMD service centre 1 from the user home network 5;

[FIG. 28] is a diagram describing a profit distribution processing operation of the EMD service centre 1;

[FIG. 29] is a diagram describing a processing operation for sending content usage record information of the EMD service centre 1 to JASRAC;

[FIG. 30] is a flowchart for describing content distribution processing;

[FIG. 31] is a flowchart for describing content distribution processing;

[FIG. 32] is a flowchart for describing the processing by which the EMD service centre 1 sends a delivery key Kd to the content provider 2;

[FIG. 33] is a flowchart for describing the cross-authentication operation between the content provider 2 and the EMD service centre 1;

[FIG. 34] is another flowchart for describing the cross-authentication operation between the content provider 2 and the EMD service centre 1;

[FIG. 35] is another flowchart for describing the cross-authentication operation between the content provider 2 and the EMD service centre 1;

[FIG. 36] is a flowchart for describing the registration processing of a receiver 51 in the EMD service centre 1;

[FIG. 37] is a diagram describing a SAM authentication certificate;

[FIG. 38] is a diagram describing a registration list;

[FIG. 39] is a flowchart illustrating the backup processing of the data of a SAM 62 in an IC card 55;

[FIG. 40] is a flowchart illustrating the backup processing of the data of a SAM 62 in an IC card 55;

[FIG. 41] is a flowchart illustrating the processing for reading backup data of the IC card 55 onto a new receiver;

[FIG. 42] is another flowchart illustrating the processing for reading backup data of the IC card 55 onto a new receiver;

[FIG. 43] is a flowchart illustrating the processing by which the receiver 51 registers a subordinate recorder 53 in the EMD service centre 1;

[FIG. 44] is a flowchart illustrating the processing by which the receiver 51 receives a delivery key Kd from the EMD service centre 1;

[FIG. 45] is a flowchart illustrating the processing for receipt of a delivery key Kd by a recorder;

[FIG. 46] is a flowchart illustrating the processing by which the content provider 2 sends a content provider secure container to the service provider 3;

[FIG. 47] is another flowchart for illustrating the processing by which the content provider 2 sends a content provider secure container to the service provider 3;

[FIG. 48] is a flowchart describing the processing by which the service provider 3 sends a service provider secure container to the receiver 51;

[FIG. 49] is a flowchart describing the processing by which the service provider 3 sends a service provider secure container to the receiver 51;

[FIG. 50] is a flowchart describing the fee processing of the receiver 51;

[FIG. 51] is a flowchart describing the processing by which the receiver 51 generates content; and

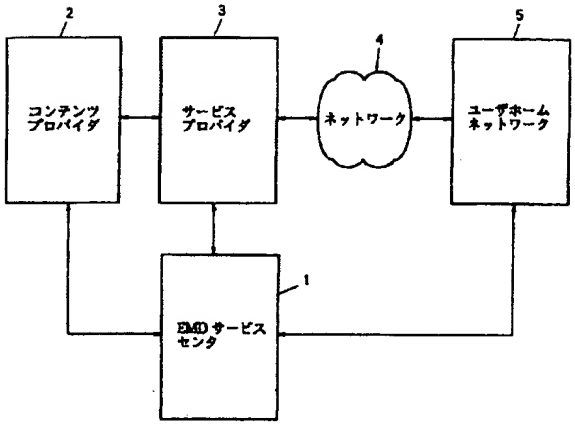
[FIG. 52] is a flowchart describing the processing by which the receiver 51 reproduces content in a decoder 56.

[Explanation of Symbols]

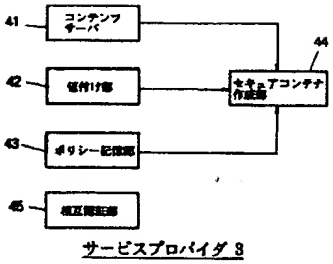
1 EMD service centre, 2 Content provider, 3 Service provider, 5 User home network, 16 Profit distribution portion, 18 User managing portion, 42 Pricing portion, 51 Receiver, 56 Decoder, 61 Communicating portion, 62

SAM, 63 Expanding portion, 71 Cross-authentication module, 72 Fee processing module, 73 Storage module, 74 Encryption/Decryption module, 75 Cross-authentication module, 76 Decryption module, 77 Decryption module, 81 Cross-authentication module, 91 Decryption unit, 92 Encryption unit, 93 Encryption unit, 101 Cross-authentication module, 102 Decryption module, 103 Decryption module.

【図１】

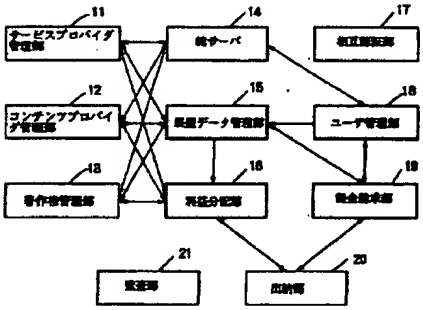


【図９】



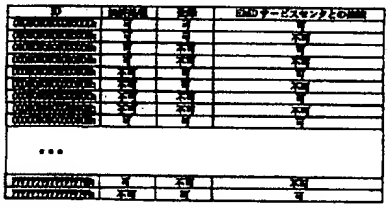
サービスプロバイダ 3

【図２】

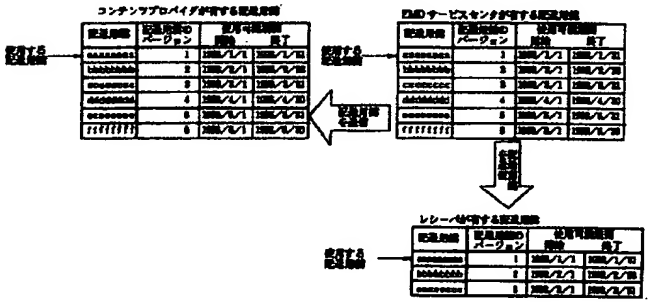


EMDサービスセンタ 1

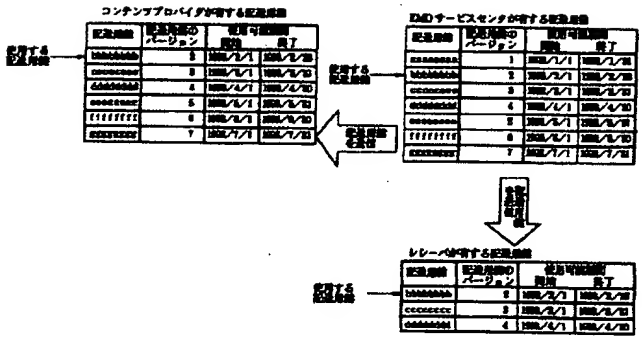
【図７】



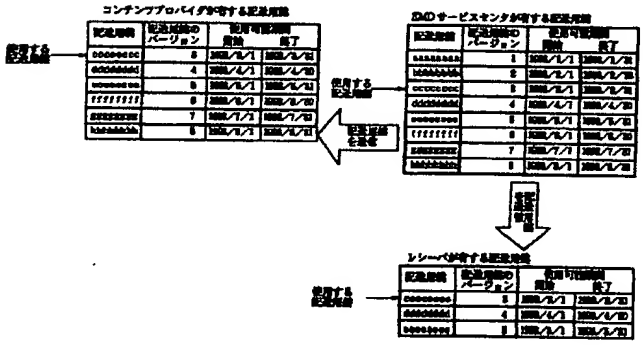
【図３】



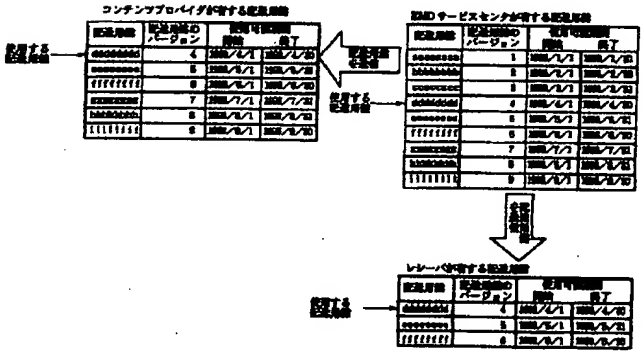
【図４】



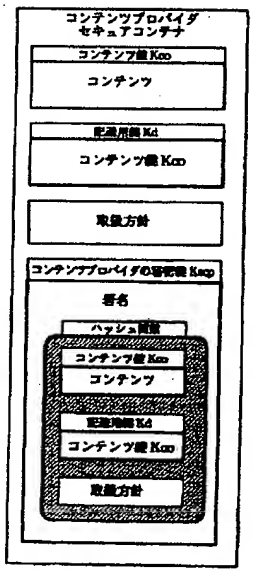
【図５】



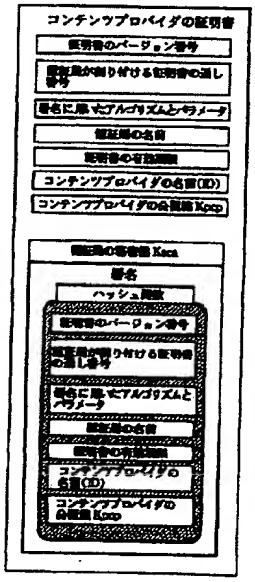
【図６】



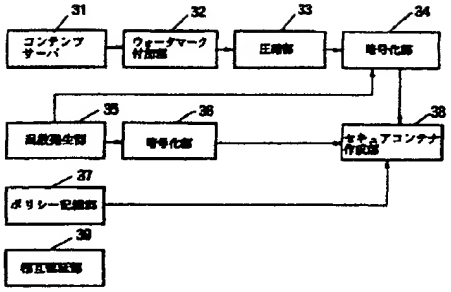
【図１３】



【図１４】

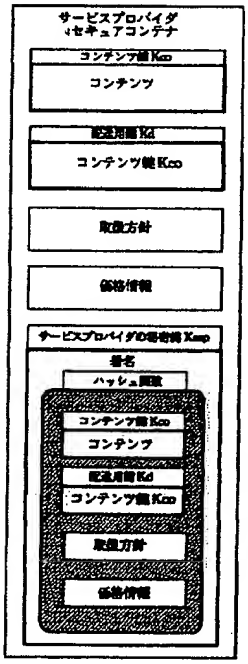


【図８】

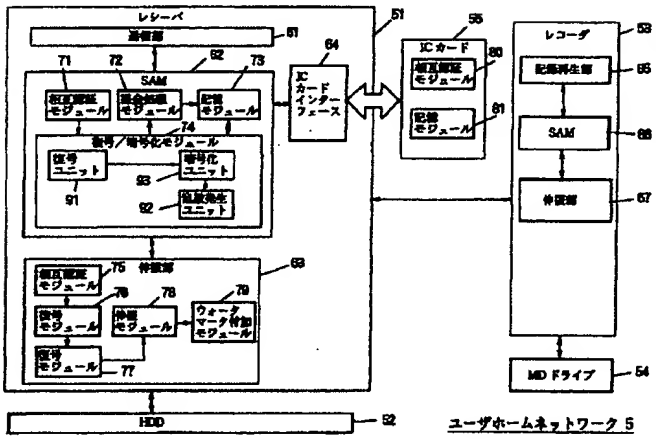


コンテンツプロバイダ 2

【図１５】

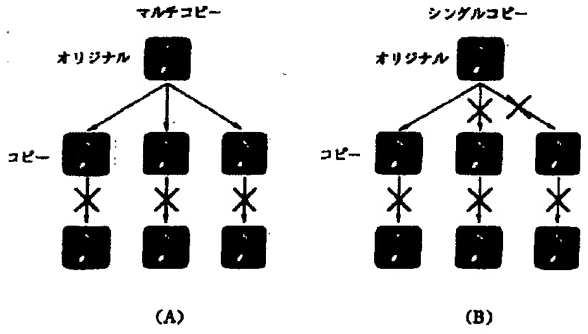


【図１０】



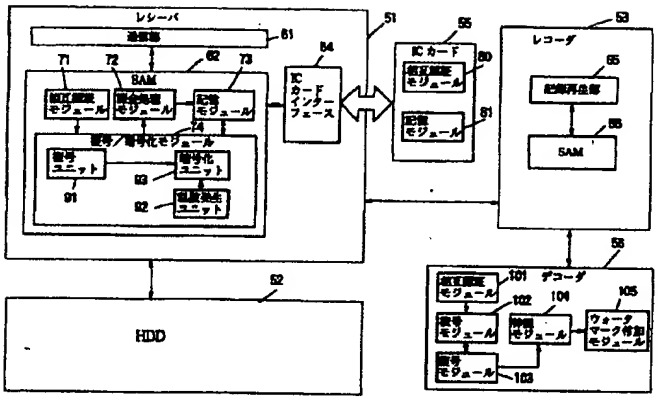
ユーザホームネットワーク 5

【図１８】



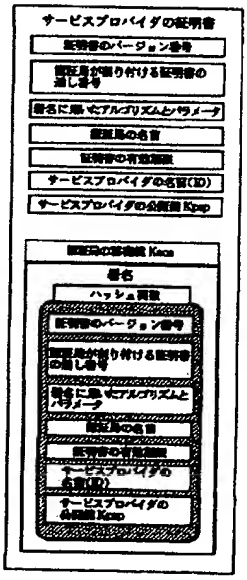
(A)　(B)

【図１１】

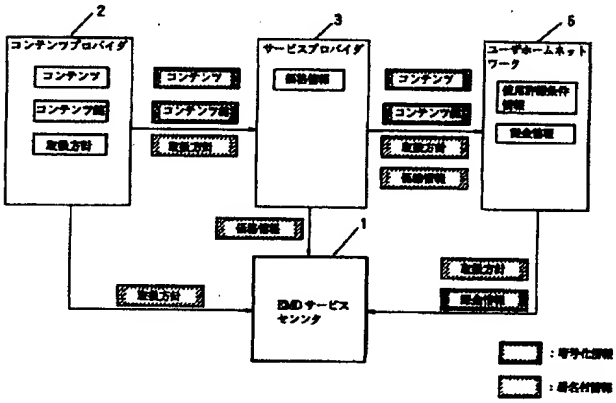


ユーザホームネットワーク 5

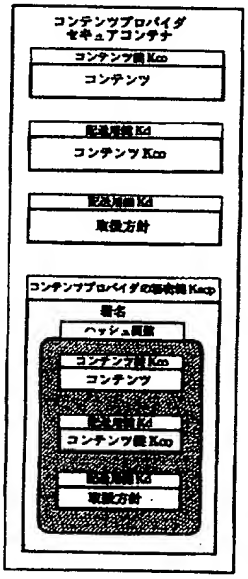
【図１６】



【図１２】



【図２５】



【図１７】

(A) 取扱方針

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1

(B) 取扱方針および価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
価格	150円	－	80円

(C) 使用許諾条件情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	0

【図１９】

(A) 取扱方針利益分配

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	70円	－	40円

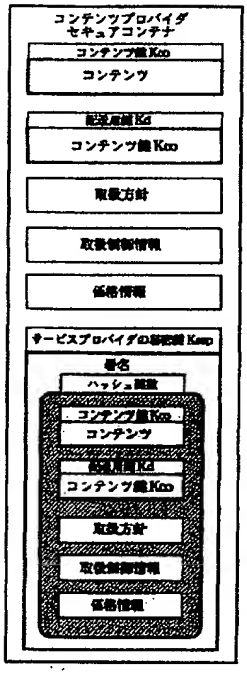
(B) 取扱方針利益分配価格情報

利用内容	再生	シングルコピー	マルチコピー
可／否	1	0	1
利益分配	60円	－	30円
分配価格	150円	－	80円

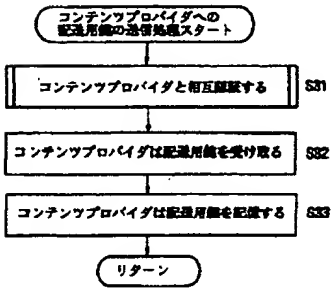
(C) 課金情報

利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

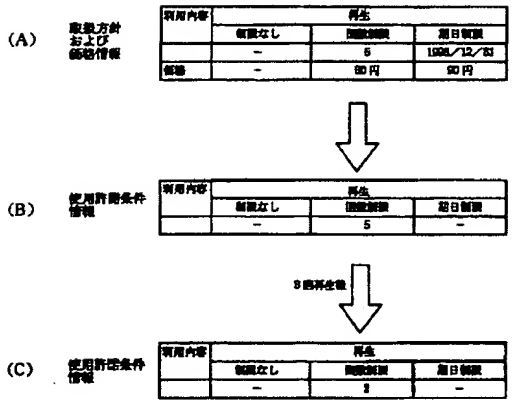
【図２２】



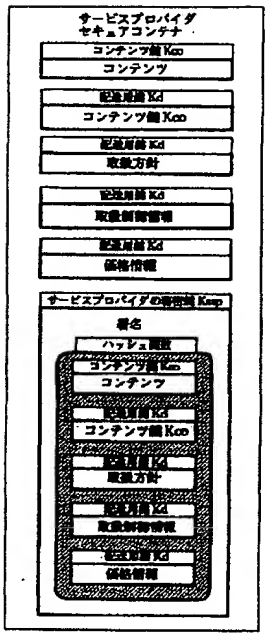
【図３２】



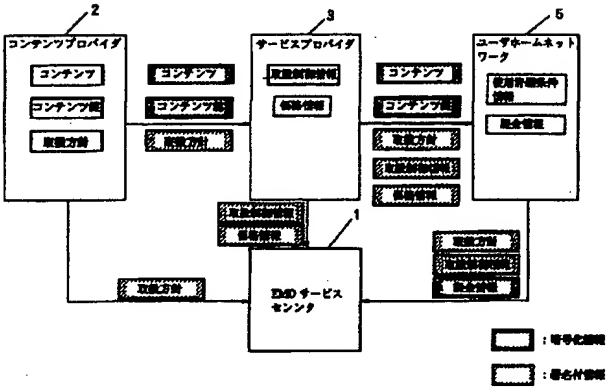
【図２０】



【図２６】



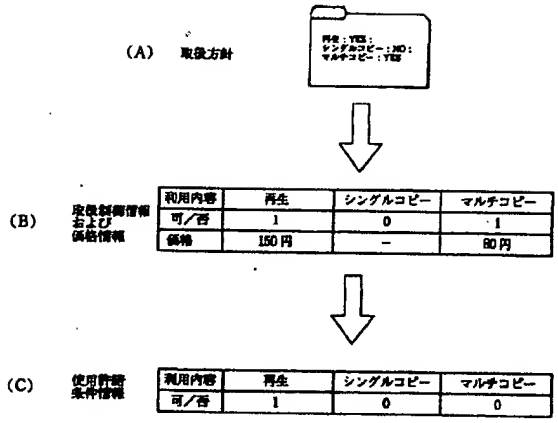
【図２１】



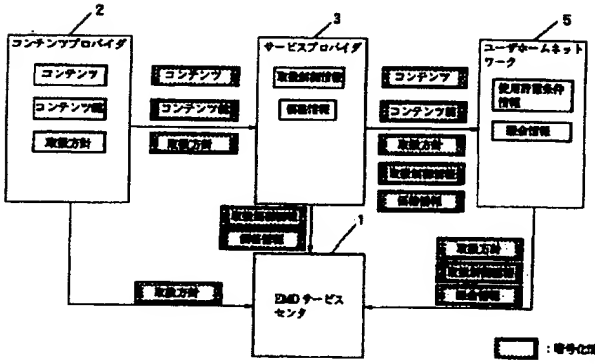
【図３８】

SAMのID (64bit)	登録状態フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

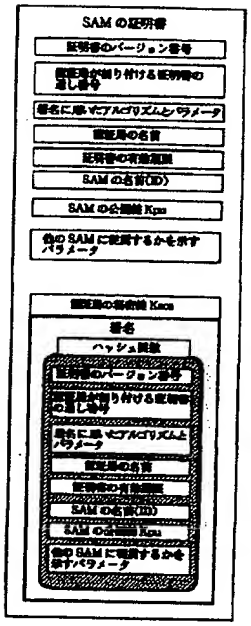
【図２３】



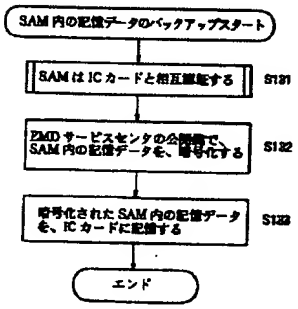
【図２４】



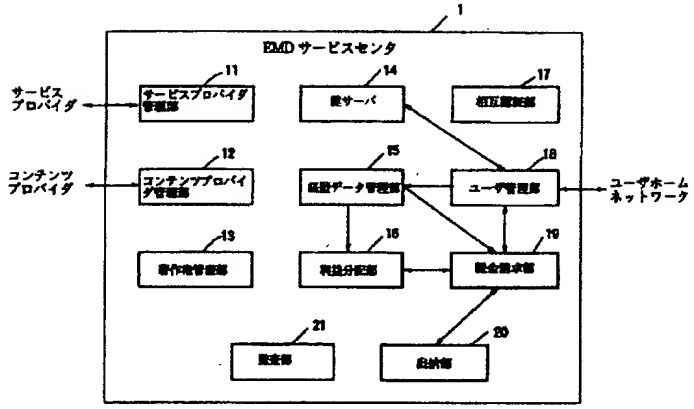
【図３７】



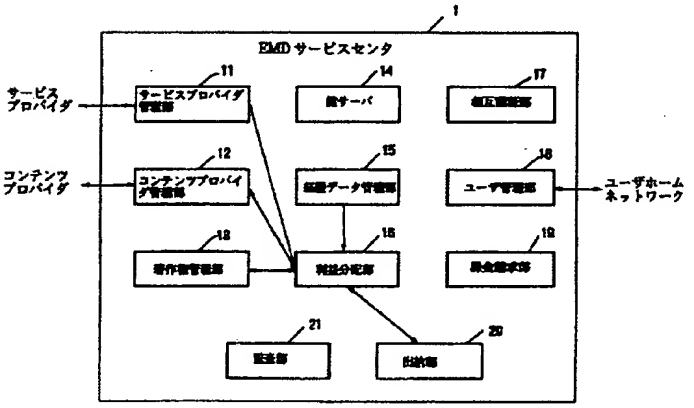
【図４０】



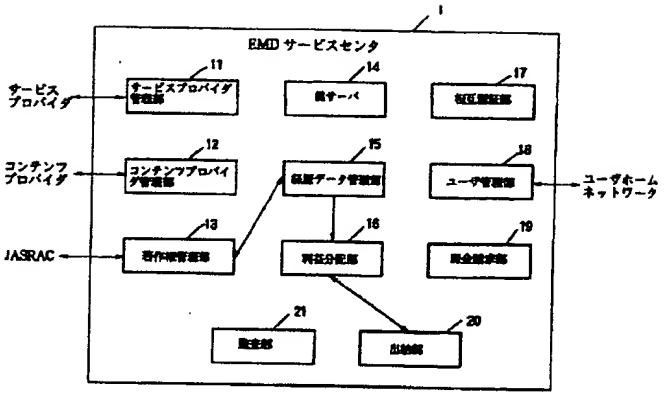
【図２７】


1
EMD サービスセンタ
サービス
プロバイダ
コンテンツ
プロバイダ
ユーザホーム
ネットワーク
11
12
13
14
15
16
17
18
19
20
21

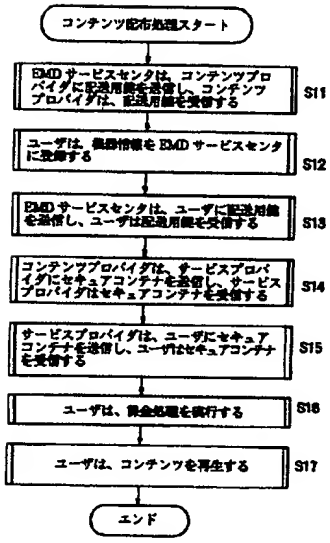
【図２８】


1
EMD サービスセンタ
サービス
プロバイダ
コンテンツ
プロバイダ
ユーザホーム
ネットワーク
11
12
13
14
15
16
17
18
19
20
21

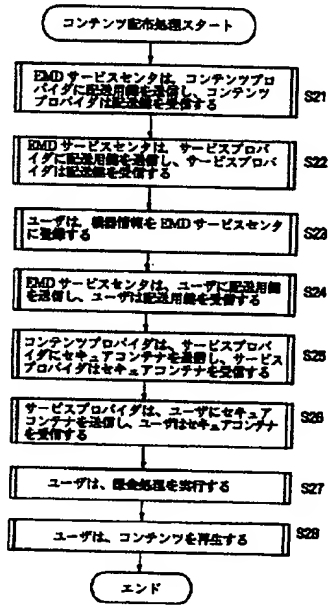
【図２９】


1
EMD サービスセンタ
11
サービスプロバイダ管理部
14
鍵サーバ
17
相互認証部
サービスプロバイダ
12
コンテンツプロバイダ管理部
15
課金データ管理部
18
ユーザ管理部
ユーザホームネットワーク
コンテンツプロバイダ
13
著作権管理部
16
再生分配部
19
課金請求部
JASRAC
21
販売部
20
出荷部

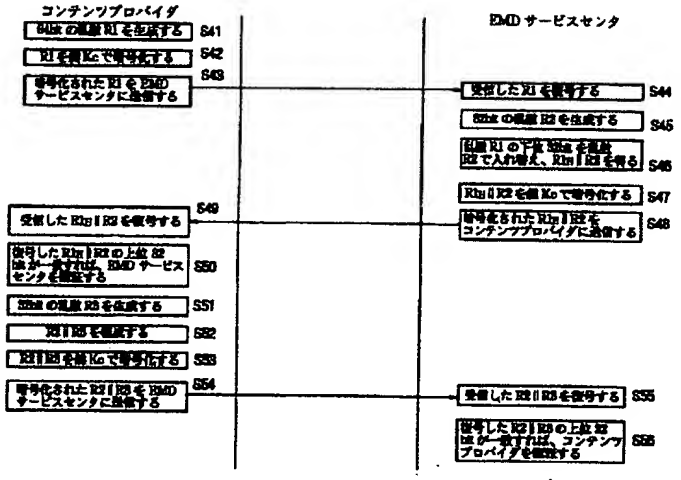
【図３０】


コンテンツ配布処理スタート
EMDサービスセンタは、コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは、配送用鍵を受信する
S11
ユーザは、機器情報をEMDサービスセンタに登録する
S12
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S13
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S14
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S15
ユーザは、課金処理を実行する
S16
ユーザは、コンテンツを再生する
S17
エンド

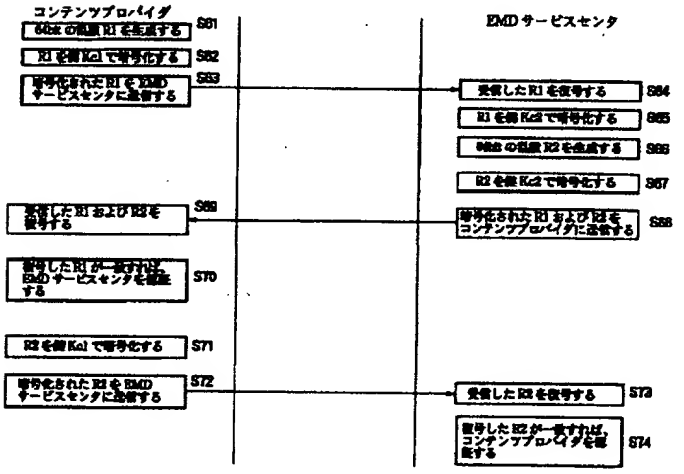
【図３１】


コンテンツ配布処理スタート
EMDサービスセンタは、コンテンツプロバイダに配送用鍵を送信し、コンテンツプロバイダは配送鍵を受信する
S21
EMDサービスセンタは、サービスプロバイダに配送用鍵を送信し、サービスプロバイダは配送鍵を受信する
S22
ユーザは、機器情報をEMDサービスセンタに登録する
S23
EMDサービスセンタは、ユーザに配送用鍵を送信し、ユーザは配送用鍵を受信する
S24
コンテンツプロバイダは、サービスプロバイダにセキュアコンテナを送信し、サービスプロバイダはセキュアコンテナを受信する
S25
サービスプロバイダは、ユーザにセキュアコンテナを送信し、ユーザはセキュアコンテナを受信する
S26
ユーザは、課金処理を実行する
S27
ユーザは、コンテンツを再生する
S28
エンド

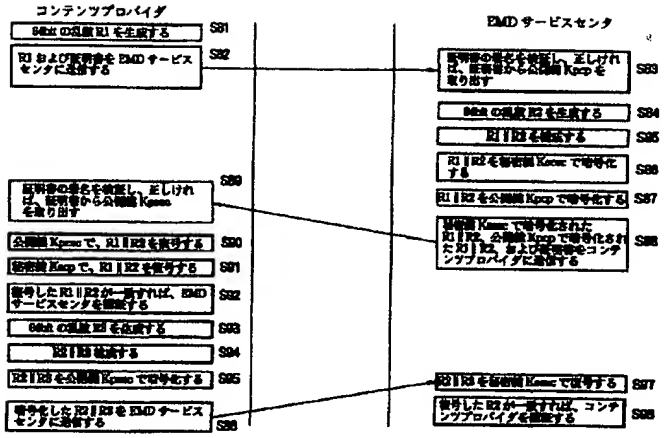
【図３３】


コンテンツプロバイダ
64bit の乱数 R1 を生成する
S41
R1 を鍵 Kc で暗号化する
S42
暗号化された R1 を EMD サービスセンタに送信する
S43
EMD サービスセンタ
受信した R1 を復号する
S44
64bit の乱数 R2 を生成する
S45
S46
R1 || R2 を鍵 Ko で暗号化する
S47
受信した R1 || R2 を復号する
S49
暗号化された R1 || R2 を コンテンツプロバイダに送信する
S48
S50
64bit の乱数 R3 を生成する
S51
R2 || R3 を結合する
S52
R2 || R3 を鍵 Ko で暗号化する
S53
暗号化された R2 || R3 を EMD サービスセンタに送信する
S54
受信した R2 || R3 を復号する
S55
S56

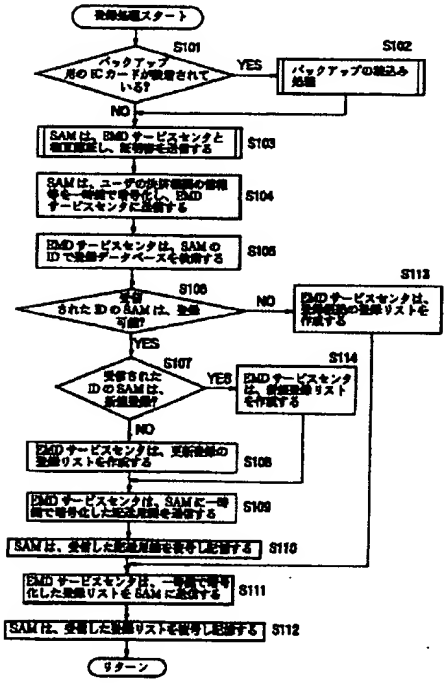
【図３４】


コンテンツプロバイダ
64bit の乱数 R1 を生成する
S61
R1 を鍵 Kc1 で暗号化する
S62
暗号化された R1 を EMD サービスセンタに送信する
S63
EMD サービスセンタ
受信した R1 を復号する
S64
R1 を鍵 Kc2 で暗号化する
S65
64bit の乱数 R2 を生成する
S66
R2 を鍵 Kc2 で暗号化する
S67
S69
暗号化された R1 および R2 をコンテンツプロバイダに送信する
S68
S70
R2 を鍵 Kc1 で暗号化する
S71
暗号化された R2 を EMD サービスセンタに送信する
S72
受信した R2 を復号する
S73
S74

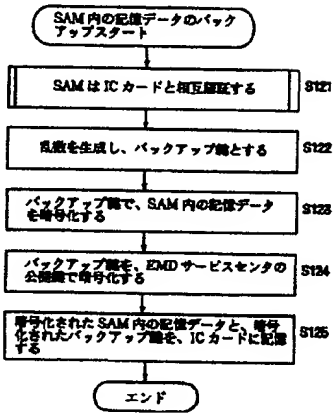
【図３５】


コンテンツプロバイダ
EMD サービスセンタ
S81
S82
S83
S84
S85
S86
S87
S88
S89
S90
S91
S92
S93
S94
S95
S96
S97
S98

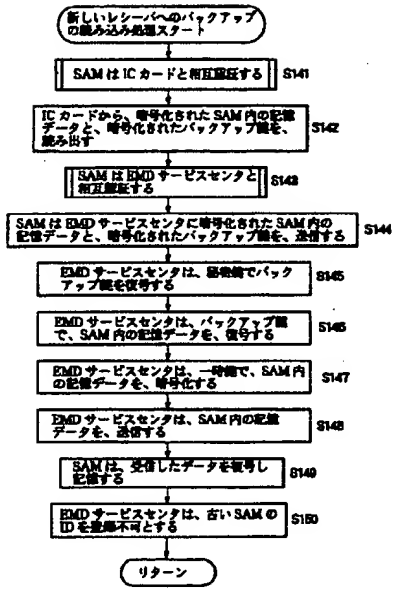
【図３６】


S101
S102
YES
NO
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
YES
NO

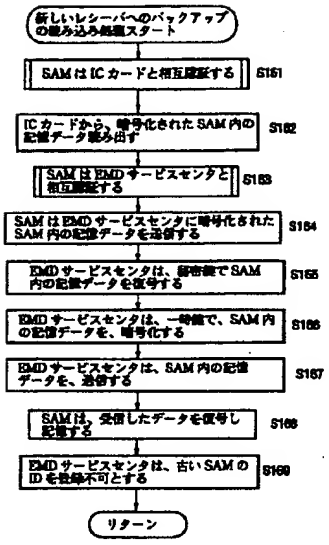
【図３９】


SAM 内の記憶データのバックアップスタート
SAM は IC カードと相互認証する
S121
乱数を生成し、バックアップ鍵とする
S122
バックアップ鍵で、SAM 内の記憶データを暗号化する
S123
バックアップ鍵を、EMD サービスセンタの公開鍵で暗号化する
S124
暗号化された SAM 内の記憶データと、暗号化されたバックアップ鍵を、IC カードに記録する
S125
エンド

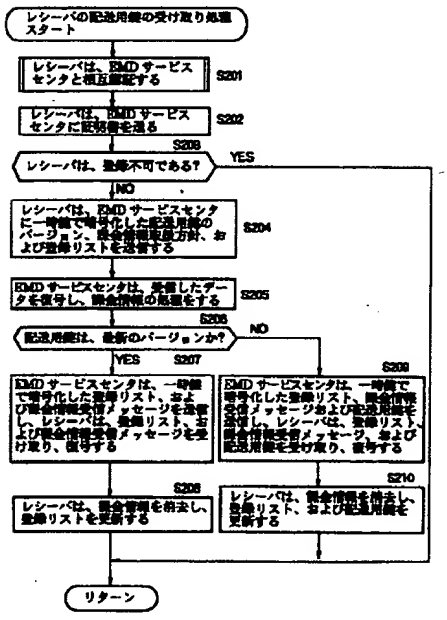
【図４１】



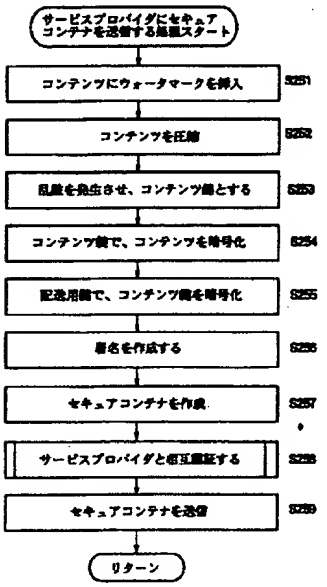
【図４２】



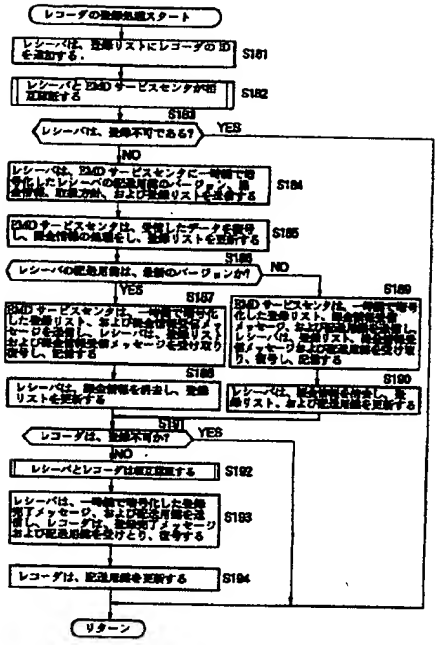
【図４４】



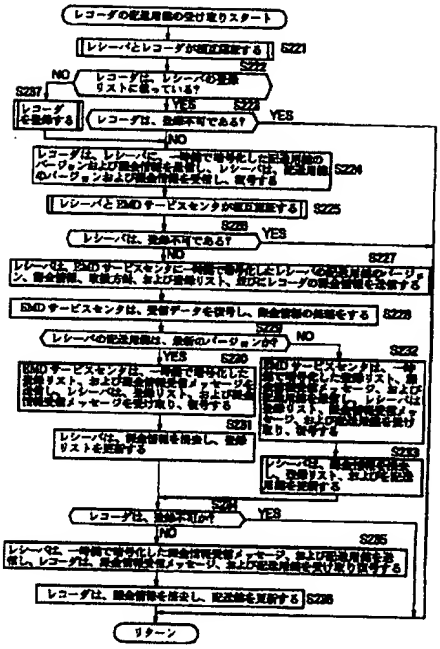
【図４６】



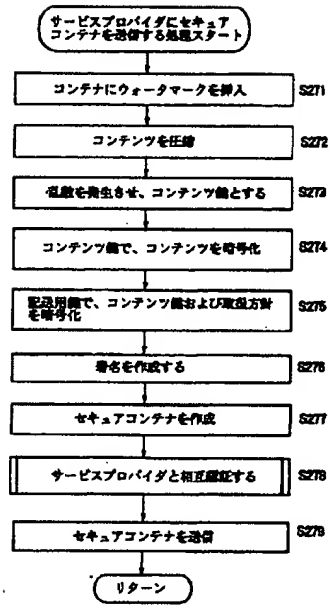
【図４３】


レコーダの登録処理スタート
S181
S182
S183
YES
NO
S184
S185
S186
NO
YES
S187
S189
S188
S190
S191
YES
NO
S192
S193
S194
リターン

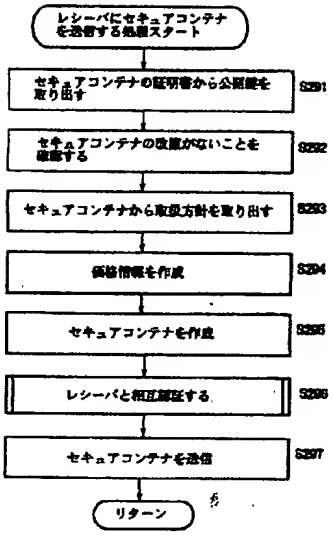
【図４５】


レコーダの視聴履歴の受け渡しスタート
S221
S222
NO
YES
S237
S223
YES
NO
S224
S225
S226
YES
NO
S227
S228
S229
NO
YES
S230
S232
S231
S233
S234
YES
NO
S235
S236
リターン

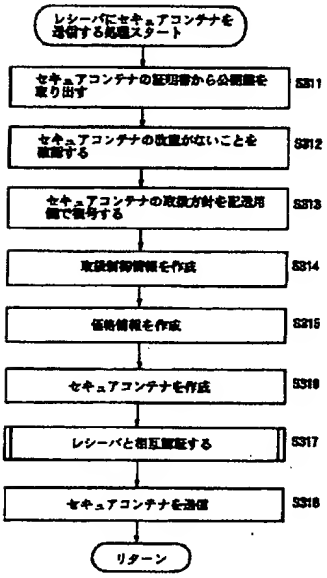
【図４７】



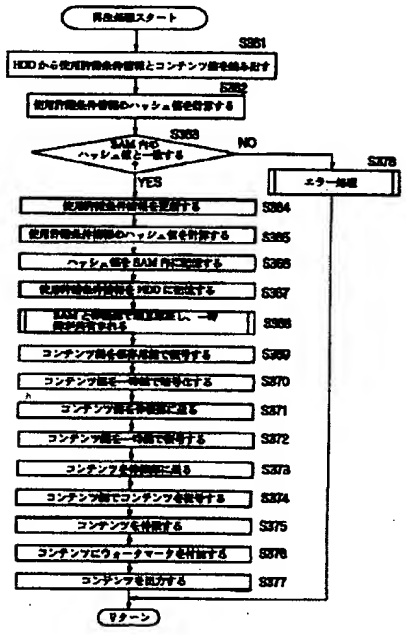
【図４８】



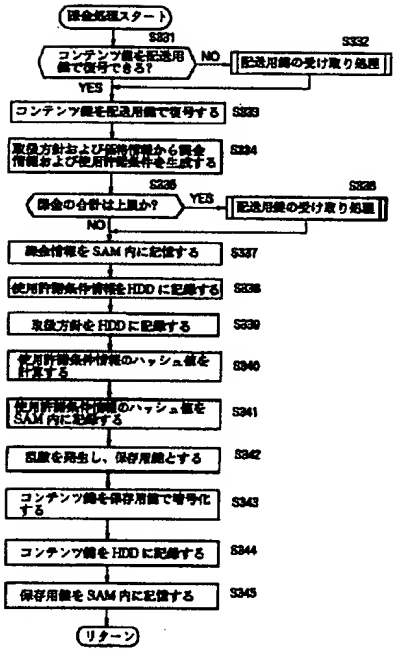
【図４９】



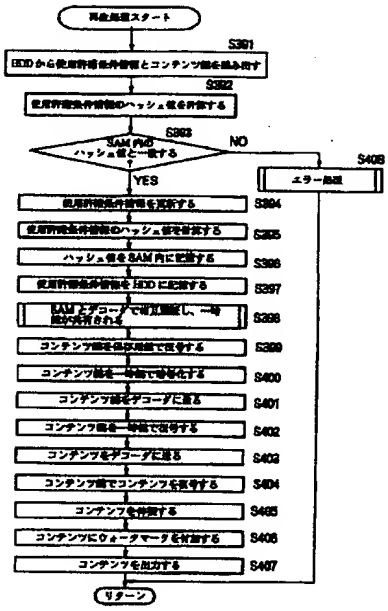
【図５１】



【図５０】


課金処理スタート
S331
コンテンツ鍵を配送用鍵で復号できる?
NO
S332
配送用鍵の受け取り処理
YES
コンテンツ鍵を配送用鍵で復号する
S333
取扱方針および課金情報から課金情報および使用許諾条件を生成する
S334
S335
課金の合計は上限か?
YES
S336
配送用鍵の受け取り処理
NO
課金情報をSAM内に記録する
S337
使用許諾条件情報をHDDに記録する
S338
取扱方針をHDDに記録する
S339
使用許諾条件情報のハッシュ値を計算する
S340
使用許諾条件情報のハッシュ値をSAM内に記録する
S341
乱数を発生し、保存用鍵とする
S342
コンテンツ鍵を保存用鍵で暗号化する
S343
コンテンツ鍵をHDDに記録する
S344
保存用鍵をSAM内に記録する
S345
リターン

【図５２】


再生処理スタート
S391
HDDから使用許諾条件情報とコンテンツ鍵を読み出す
S392
使用許諾条件情報のハッシュ値を計算する
S393
SAM内のハッシュ値と一致する
NO
S408
エラー処理
YES
使用許諾条件情報を復号する
S394
使用許諾条件情報のハッシュ値を計算する
S395
ハッシュ値をSAM内に記録する
S396
使用許諾条件情報をHDDに記録する
S397
SAMとデコーダで相互認証し、一時鍵が共有される
S398
コンテンツ鍵を保存用鍵で復号する
S399
コンテンツ鍵を一時鍵で暗号化する
S400
コンテンツ鍵をデコーダに送る
S401
コンテンツ鍵を一時鍵で復号する
S402
コンテンツをデコーダに送る
S403
コンテンツ鍵でコンテンツを復号する
S404
コンテンツを伸張する
S405
コンテンツにウォータマークを付加する
S406
コンテンツを出力する
S407
リターン

Key to figures

[FIG. 1]

2 CONTENT PROVIDER
3 SERVICE PROVIDER
4 NETWORK
5 USER HOME NETWORK
1 EMD SERVICE CENTRE

[FIG. 9]

41 CONTENT SERVER
42 PRICING PORTION
43 POLICY STORING PORTION
45 CROSS-AUTHENTICATING PORTION
44 SECURE CONTAINER PRODUCING PORTION
SERVICE PROVIDER 3

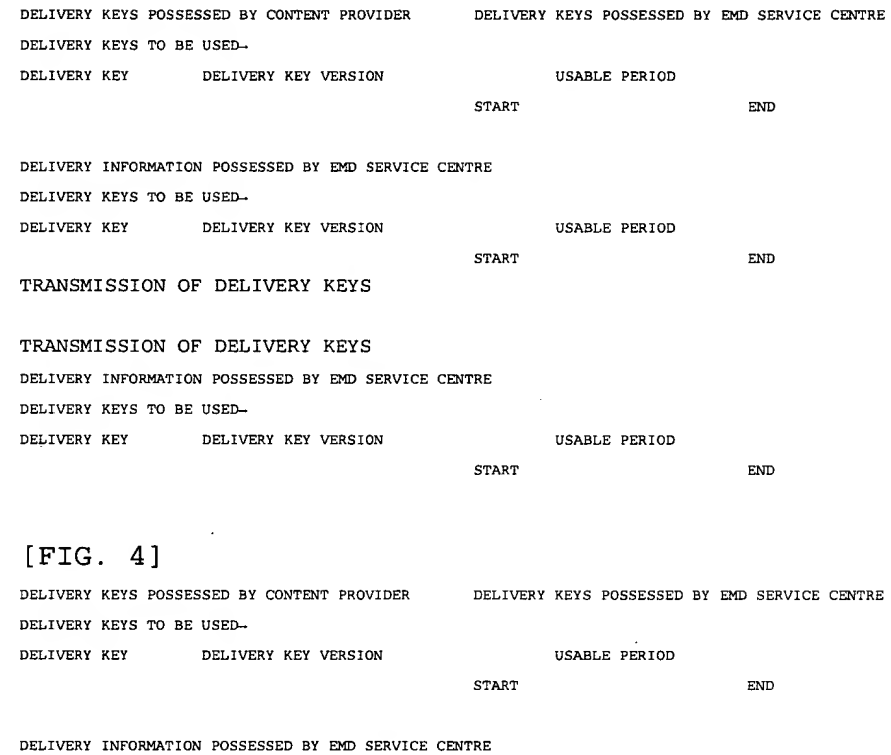
[FIG. 2]

11 SERVICE PROVIDER MANAGING PORTION
12 CONTENT PROVIDER MANAGING PORTION
13 COPYRIGHT MANAGING PORTION
14 KEY SERVER
15 LOG DATA MANAGING PORTION
16 PROFIT DISTRIBUTION PORTION
17 CROSS-AUTHENTICATING PORTION
18 USER MANAGING PORTION
19 BILLING PORTION
21 AUDITING PORTION
20 ACCOUNTING PORTION
EMD SERVICE CENTRE 1

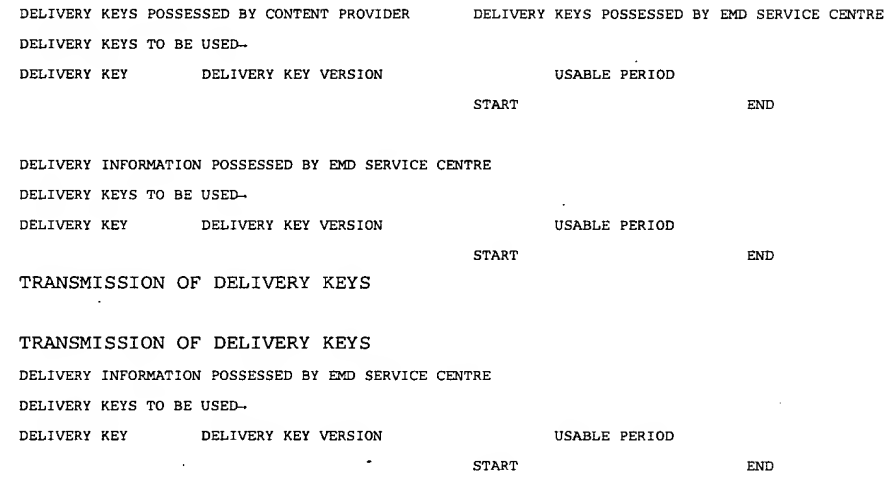
[FIG. 7]

SETTLEMENT PROCESSING	REGISTRATION	CONNECTION WITH EMD SERVICE CENTRE
YES	YES	YES
YES	YES	NO
YES	NO	YES
YES	NO	NO
NO	YES	YES
NO	YES	NO
NO	NO	YES
NO	NO	NO
YES	YES	YES
YES	NO	NO
NO	YES	YES

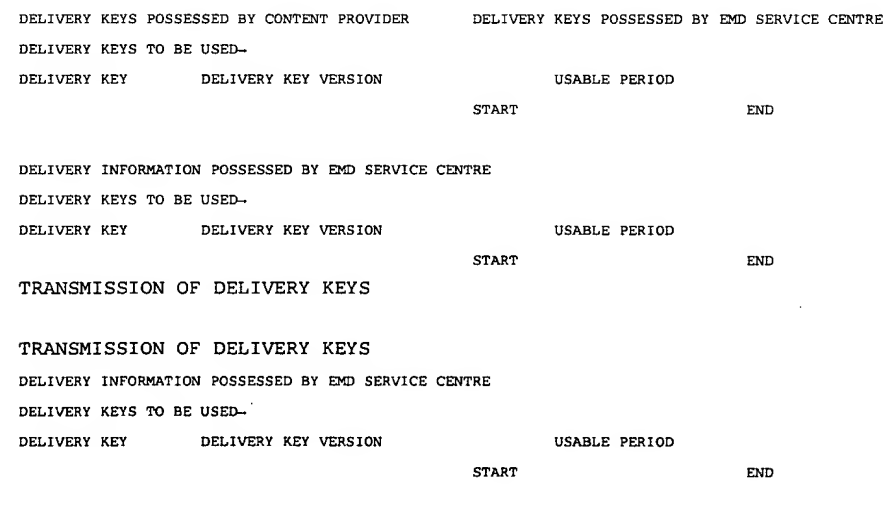
[FIG. 3]



[FIG. 4]



[FIG. 5]



[FIG. 6]

[FIG. 13]

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY
CONTENT PROVIDER SECRET KEY Kscp
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY

[FIG. 14]

CONTENT PROVIDER AUTHENTICATION CERTIFICATE
AUTHENTICATION CERTIFICATE VERSION NO.
AUTHENTICATION CERTIFICATE SERIAL NUMBER ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS EMPLOYED IN SIGNATURE
CERTIFYING AGENCY NAME
AUTHENTICATION CERTIFICATE PERIOD OF VALIDITY
CONTENT PROVIDER NAME (ID)
CONTENT PROVIDER PUBLIC KEY Kpcp
CERTIFYING AGENCY SECRET KEY Ksca
SIGNATURE
HASH FUNCTION
AUTHENTICATION CERTIFICATE VERSION NO.
AUTHENTICATION CERTIFICATE SERIAL NO.
ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS
EMPLOYED IN SIGNATURE
CERTIFYING AGENCY NAME
AUTHENTIFICATION CERTIFICATE
PERIOD OF VALIDITY
CONTENT PROVIDER NAME (ID)
CONTENT PROVIDER PUBLIC KEY Kpcp

[FIG. 8]

31 CONTENT SERVER
32 WATERMARKING PORTION
33 COMPRESSING PORTION
34 ENCRYPTING PORTION
35 RANDOM NUMBER GENERATING PORTION
36 ENCRYPTING PORTION
38 SECURE CONTAINER PRODUCING PORTION
37 POLICY STORING PORTION
39 CROSS-AUTHENTICATING PORTION
CONTENT PROVIDER 2

[FIG. 15]

SERVICE PROVIDER SECURE CONTAINER
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY
PRICING INFORMATION
SERVICE PROVIDER SECRET KEY Kscp
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY
PRICING INFORMATION

[FIG. 10]

51 RECEIVER
COMMUNICATING PORTION 61
SAM 62
CROSS-AUTHENTICATION MODULE 71
FEE MODULE 72
STORAGE MODULE 73
DECRYPTION/ENCRYPTION MODULE 74
DECRYPTION UNIT 91
ENCRYPTION MODULE 93
RANDOM NUMBER GENERATING UNIT 92
EXPANSION PORTION 63
CROSS-AUTHENTICATION MODULE 75
DECRYPTION MODULE 76
DECRYPTION MODULE 77
EXPANSION MODULE 78
WATERMARKING MODULE 79
HDD52
IC CARD INTERFACE 64
IC CARD 55
CROSS-AUTHENTICATION MODULE 80
STORAGE MODULE 81
RECORDER 53
RECORDING/REPRODUCING PORTION 65
SAM 66
EXPANDING PORTION 67
MD DRIVER 54

USER HOME NETWORK 5

[FIG. 18]

MULTIPLE COPY

ORIGINAL

COPY

SINGLE COPY

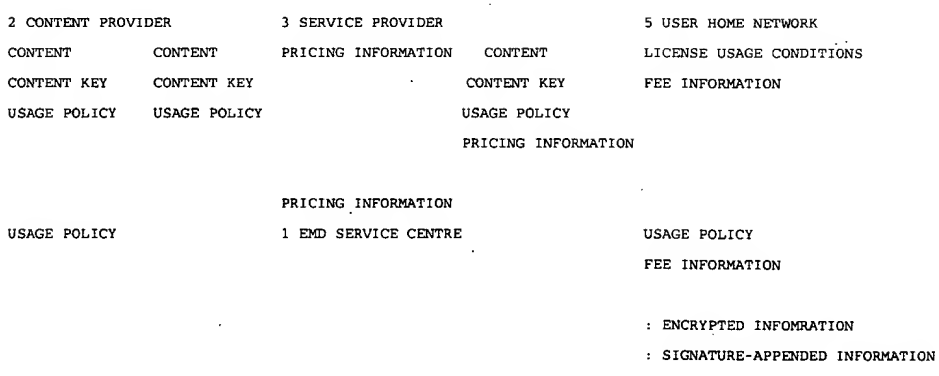
ORIGINAL

COPY

[FIG. 11]

51 RECEIVER
COMMUNICATING PORTION 61
SAM 62
CROSS-AUTHENTICATION MODULE 71
FEE MODULE 72
STORAGE MODULE 73
DECRYPTION/ENCRYPTION MODULE 74
DECRYPTION UNIT 91
ENCRYPTION MODULE 93
ENCRYPTION UNIT 92
HDD 52
IC CARD INTERFACE 64
55 IC CARD
CROSS-AUTHENTICATION MODULE 80
STORAGE MODULE 81
53 RECEIVER
RECORDING/REPRODUCING PORTION 65
SAM 66
56 DECODER
CROSS-AUTHENTICATION MODULE 101
DECRYPTION MODULE 102
EXPANSION MODULE 104
DECCRYPTION MODULE 103
WATERMARKING MODULE 105
USER HOME NETWORK 5

[FIG. 12]



[FIG. 16]

SERVICE PROVIDER AUTHENTICATION CERTIFICATE
AUTHENTICATION CERTIFICATE VERSION NO.
SERIAL NO. ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS EMPLOYED IN SIGNATURE
CERTIFYING AGENCY NAME
AUTHENTICATION CERTIFICATE PERIOD OF VALIDITY
SERVICE PROVIDER NAME (ID)
SERVICE PROVIDER PUBLIC KEY Kpsp
CERTIFYING AGENCY SECRET KEY Ksca
SIGNATURE
HASH FUNCTION
AUTHENTICATION CERTIFICATE VERSION NO.
SERIAL NO. ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS EMPLOYED IN SIGNATURE
CERTIFYING AGENCY NAME
AUTHENTICATION CERTIFICATE PERIOD OF VALIDITY
SERVICE PROVIDER NAME (ID)
SERVICE PROVIDER PUBLIC KEY Kpsp

[FIG. 25]

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
DELIVERY KEY Kd
USAGE POLICY
CONTENT PROVIDER (SIC) SECRET KEY Kscp
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
DELIVERY KEY Kd
USAGE POLICY

[FIG. 22]

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY
USAGE CONTROL INFORMATION
PRICING INFORMATION
SERVICE PROVIDER SECRET KEY Kscp
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
USAGE POLICY
USAGE CONTROL INFORMATION
PRICING INFORMATION

[FIG. 17]

(A) USAGE POLICY

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

YES/NO

(B) USAGE POLICY AND PRICING INFORMATION

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

YES/NO

PRICE

(C) LICENSE USAGE CONDITIONS

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

YES/NO

[FIG. 19]

(A) USAGE POLICY, PROFIT SHARING

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

YES/NO

PROFIT SHARING

(B) USAGE POLICY, PROFIT SHARING, PRICING INFORMATION

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

YES/NO

PROFIT SHARING

SHARED PRICE

(C) FEE INFORMATION

USAGE DETAILS REPRODUCTION SINGLE COPY MULTIPLE COPY

USE FREQUENCY

[FIG. 32]

START DELIVERY KEY TRANSMISSION PROCESSING TO CONTENT PROVIDER

CROSS-AUTHENTICATION WITH CONTENT PROVIDER S31

RECEIPT OF DELIVERY KEY BY CONTENT PROVIDER S32

STORAGE OF DELIVERY KEY BY CONTENT PROVIDER S33

RETURN

[FIG. 26]

SERVICE PROVIDER SECURE CONTAINER
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
DELIVERY KEY Kd
USAGE POLICY
DELIVERY KEY Kd
USAGE CONTROL INFORMATION
DELIVERY KEY Kd
PRICING INFORMATION
SERVICE PROVIDER SECRET KEY Kssp
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
DELIVERY KEY Kd
USAGE POLICY
DELIVERY KEY Kd
USAGE CONTROL INFORMATION
DELIVERY KEY Kd
PRICING INFORMATION

[FIG. 20]

(A) USAGE POLICY AND PRICING INFORMATION

USAGE DETAILS	REPRODUCTION		
	NO RESTRICTION	FREQUENCY RESTRICTION	DATE RESTRICTION
PRICE			

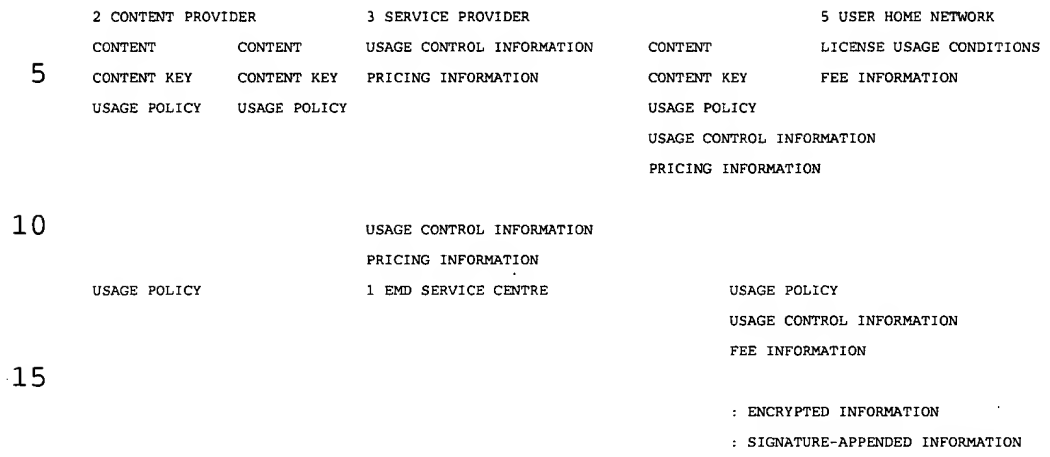
(B) LICENSE CONDITIONS INFORMATION

USAGE DETAILS	REPRODUCTION		
	NO RESTRICTION	FREQUENCY RESTRICTION	DATE RESTRICTION

(C) LICENSE CONDITIONS INFORMATION

USAGE DETAILS	REPRODUCTION		
	NO RESTRICTION	FREQUENCY RESTRICTION	DATE RESTRICTION

[FIG. 21]



[FIG. 38]

ID of SAM	REGISTRATION REFUSAL FLAG	STATUS FLAG	CONDITION FLAG	SIGNATURE
(64 bit)	(1 bit)	(4 bit)	(i bit)	

[FIG. 23]

(A) USAGE POLICY

REPRODUCTION: YES

SINGLE COPY: NO

MULTIPLE COPY: YES

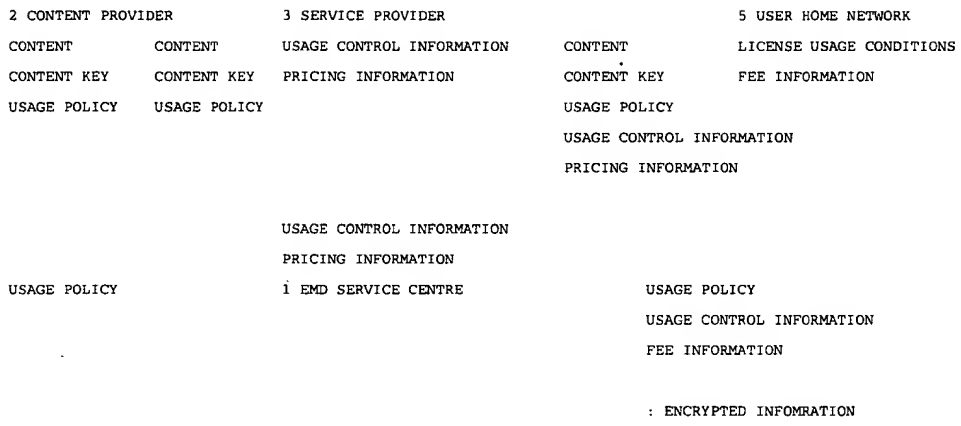
(B) USAGE CONTROL INFORMATION AND PRICING INFORMATION

USAGE DETAILS	REPRODUCTION	SINGLE COPY	MULTIPLE COPY
YES/NO			
PRICE			

(C) LICENSE USAGE CONDITIONS

USAGE DETAILS	REPRODUCTION	SINGLE COPY	MULTIPLE COPY
YES/NO			

[FIG. 24]



[FIG. 37]

SAM AUTHENTICATION CERTIFICATE
AUTHENTICATION CERTIFICATE VERSION NO.
SERIAL NO. ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS EMPLOYED IN AUTHENTICATION CERTIFICATE
CERTIFYING AGENCY NAME
AUTHENTICATION CERTIFICATE PERIOD OF VALIDITY
SAM NAME (ID)
SAM PUBLIC KEY Kpu
PARAMETERS INDICATING IF SUBORDINATE TO OTHER SAM
AUTHENTICATION CERTIFICATE SECRET KEY Ksca
SIGNATURE
HASH FUNCTION
AUTHENTICATION CERTIFICATE VERSION NO.
SERIAL NO. ASSIGNED BY CERTIFYING AGENCY
ALGORITHMS AND PARAMETERS EMPLOYED IN SIGNATURE
CERTIFYING AGENCY NAME
AUTHENTICATION CERTIFICATE PERIOD OF VALIDITY
SAM NAME (ID)
SAM PUBLIC KEY Kpu
PARAMETERS INDICATING IF SUBORDINATE TO OTHER SAM

[FIG. 40]

START SAM STORAGE DATA BACKUP

CROSS-AUTHENTICATION OF SAM WITH IC CARD S131

ENCRYPTION OF SAM STORAGE DATA WITH EMD SERVICE CENTRE PUBLIC KEY S132

STORAGE OF ENCRYPTED SAM STORAGE DATA IN IC CARD S133

END

[FIG. 27]

1 EMD SERVICE CENTRE
SERVICE PROVIDER
CONTENT PROVIDER
11 SERVICE PROVIDER MANAGING PORTION
12 CONTENT PROVIDER MANAGING PORTION
13 COPYRIGHT MANAGING PORTION
14 KEY SERVER
15 LOG DATA MANAGING PORTION
16 PROFIT DISTRIBUTION PORTION
17 CROSS-AUTHENTICATING PORTION
18 USER MANAGING PORTION
19 BILLING PORTION
20 ACCOUNTING PORTION
21 AUDITING PORTION
USER HOME NETWORK

[FIG. 28]

1 EMD SERVICE CENTRE
SERVICE PROVIDER
CONTENT PROVIDER
11 SERVICE PROVIDER MANAGING PORTION
12 CONTENT PROVIDER MANAGING PORTION
13 COPYRIGHT MANAGING PORTION
14 KEY SERVER
15 LOG DATA MANAGING PORTION
16 PROFIT DISTRIBUTION PORTION
17 CROSS-AUTHENTICATING PORTION
18 USER MANAGING PORTION
19 BILLING PORTION
20 ACCOUNTING PORTION
USER HOME NETWORK

[FIG. 29]

1 EMD SERVICE CENTRE
SERVICE PROVIDER
CONTENT PROVIDER
JASRAC
11 SERVICE PROVIDER MANAGING PORTION
12 CONTENT PROVIDER MANAGING PORTION
13 COPYRIGHT MANAGING PORTION
14 KEY SERVER
15 LOG DATA MANAGING PORTION
16 PROFIT DISTRIBUTION PORTION
17 CROSS-AUTHENTICATING PORTION
18 USER MANAGING PORTION
19 BILLING PORTION
20 ACCOUNTING PORTION
USER HOME NETWORK

[FIG. 30]

START CONTENT DISTRIBUTION PROCESSING

S11 TRANSMISSION OF DELIVERY KEY TO CONTENT PROVIDER BY EMD SERVICE CENTRE, RECEIPT OF DELIVERY KEY BY CONTENT PROVIDER

S12 REGISTRATION OF DEVICE INFORMATION IN EMD SERVICE CENTRE BY USER

S13 TRANSMISSION OF DELIVERY KEY TO USER BY EMD SERVICE CENTRE, RECEIPT OF DELIVERY KEY BY USER

S14 TRANSMISSION OF SECURE CONTAINER TO SERVICE PROVIDER BY CONTENT PROVIDER; RECEIPT OF SECURE CONTAINER BY SERVICE PROVIDER

S15 TRANSMISSION OF SECURE CONTAINER TO USER BY SERVICE PROVIDER, RECEIPT OF SECURE CONTAINER BY USER

S16 EXECUTION OF FEE PROCESSING BY USER

S17 REPRODUCTION OF CONTENT BY USER

END

[FIG. 31]

START CONTENT DISTRIBUTION PROCESSING

S21 TRANSMISSION OF DELIVERY KEY TO CONTENT PROVIDER BY EMD SERVICE CENTRE, RECEIPT OF DELIVERY KEY BY CONTENT PROVIDER

S22 TRANSMISSION OF DELIVERY KEY TO SERVICE PROVIDER BY EMD SERVICE CENTRE, RECEIPT OF DELIVERY KEY BY SERVICE PROVIDER

S23 REGISTRATION OF DEVICE INFORMATION IN EMD SERVICE CENTRE BY USER

S24 TRANSMISSION OF DELIVERY KEY TO USER BY EMD SERVICE CENTRE, RECEIPT OF DELIVERY KEY BY USER

S25 TRANSMISSION OF SECURE CONTAINER TO SERVICE PROVIDER BY CONTENT PROVIDER, RECEIPT OF SECURE CONTAINER BY SERVIDE PROVIDER

S26 TRANSMISSION OF SECURE CONTAINER TO USER BY SERVICE PROVIDER, RECEIPT OF SECURE CONTAINER BY USER

S27 EXECUTION OF FEE PROCESSING BY USER

S28 REPRODUCTION OF CONTENT BY USER

END

[FIG. 33]

CONTENT PROVIDER

S41 GENERATION OF 64 bit RANDOM NUMBER R1

S42 ENCRYPTION OF R1 WITH KEY Kc

S43 TRANSMISSION OF ENCRYPTED R1 TO EMD SERVICE CENTRE

S49 DECRYPTION OF RECEIVED $R1_H \| R2$

S50 VERIFICATION OF EMD SERVICE CENTRE IF HIGH-ORDER 32 bits MATCH DECRYPTED $R1_H \| R2$

S51 GENERATION OF 32 bit RANDOM NUMBER R3

S52 CONFIGURING OF $R2 \| R3$

S53 ENCRYPTION OF $R2 \| R3$ WITH KEY Kc

S54 TRANSMISSION OF ENCRYPTED $R2 \| R3$ TO EMD SERVICE CENTRE

EMD SERVICE CENTRE

S44 DECRYPTION OF RECEIVED R1

S45 GENERATION OF 32 bit RANDOM NUMBER R2

S46 SUBSTITUTION OF LOW-ORDER 32 bits OF RANDOM NUMBER R1 TO OBTAIN $R1_H \| R2$

S47 ENCRYPTION OF $R1_H \| R2$ WITH KEY Kc

S48 TRANSMISSION OF ENCRYPTED $R1_H \| R2$ TO CONTENT PROVIDER

S55 ENCRYPTION OF RECEIVED $R2 \| R3$

S56 VERIFICATION OF CONTENT PROVIDER IF HIGH-ORDER 32 bits MATCH DECRYPTED $R2 \| R3$

[FIG. 34]

CONTENT PROVIDER

S61 GENERATION OF 64 bit RANDOM NUMBER R1

S62 ENCRYPTION OF R1 WITH KEY Kc1

S63 TRANSMISSION OF ENCRYPTED R1 TO EMD SERVICE CENTRE

S69 DECRYPTION OF RECEIVED R1 and R2

S70 VERIFICATION OF EMD SERVICE CENTRE IF MATCH WITH DECRYPTED R1

S71 ENCRYPTION OF R2 WITH KEY Kc1

S72 TRANSMISSION OF ENCRYPTED R2 TO EMD SERVICE CENTRE

EMD SERVICE CENTRE

S64 DECRYPTION OF RECEIVED R1

S65 ENCRYPTION OF R1 WITH KEY Kc1

S66 GENERATION OF 64 bit RANDOM NUMBER R2

S67 ENCRYPTION OF R2 with KEY Kc2

S68 TRANSMISSION OF ENCRYPTED R1 AND R2 TO CONTENT PROVIDER

S73 DECRYPTION OF RECEIVED R2

S74 VERIFICATION OF CONTENT PROVIDER IF MATCH WITH DECRYPTED R2

[FIG. 33]

CONTENT PROVIDER

S81 GENERATION OF 64 bit RANDOM NUMBER R1

S82 TRANSMISSION OF R1 AND AUTHENTICATION CERTIFICATE TO EMD SERVICE CENTRE

S89 CHECK OF AUTHENTICATION CERTIFICATE SIGNATURE AND, IF LEGITIMATE, EXTRACTION OF PUBLIC KEY Kpesc FROM AUTHENTICATION CERTIFICATE

S90 DECRYPTION OF R1‖R2 WITH PUBLIC KEY Kpeac

S91 DECRYPTION OF R1‖R2 WITH PUBLIC KEY Kspc

S92 VERIFICATION OF EMD SERVICE CENTRE IF MATCH WITH DECRYPTED R1‖R2

S93 GENERATION OF 64 bit RANDOM NUMBER R3

S94 CONFIGURING OF R2‖R3

S95 ENCRYPTION OF R2‖R3 WITH PUBLIC KEY Kpeac

S96 TRANSMISSION OF ENCRYPTED R2‖R3 TO EMD SERVICE CENTRE

EMD SERVICE CENTRE

S83 CHECK OF AUTHENTICATION CERTIFICATE SIGNATURE AND, IF LEGITIMATE, EXTRACTION OF PUBLIC KEY Kpcp FROM AUTHENTICATION CERTIFICATE

S84 GENERATION OF 64 bit RANDOM NUMBER R2

S85 CONFIGURING OF R1‖R2

S86 ENCRYPTION OF $R1_H$‖R2 WITH SECRET KEY Ksesc

S87 ENCRYPTION OF $R1_H$‖R2 WITH PUBLIC KEY Kpcp

S88 TRANSMISSION OF R1‖R2 ENCRYPTED WITH SECRET KEY Ksesc, R1‖R2 ENCRYPTED WITH PUBLIC KEY Kpcp AND AUTHENTICATION CERTIFICATE TO CONTENT PROVIDER

S97 DECRYPTION OF R1‖R2 WITH SECRET KEY Ksesc

S98 VERIFICATION OF CONTENT PROVIDER IF MATCH WITH DECRYPTED R2

[FIG. 36]

START REGISTRATION PROCESSING
S101 IS BACKUP IC CARD LOADED?
S102 BACKUP READ PROCESSING
S103 CROSS-AUTHENTICATION WITH EMD SERVICE CENTRE AND TRANSMISSION OF AUTHENTICATION CERTIFICATE BY SAM
S104 ENCRYPTION OF INFORMATION SUCH AS USER SETTLEMENT AGENCY AND TRANSMISSION THEREOF TO EMD SERVICE CENTRE BY SAM
S105 SEARCH OF REGISTRATION DATABASE BY EMD SERVICE CENTRE BASED ON SAM ID
S106 SAM OF RECEIVED ID ABLE TO BE REGISTERED?
S113 PRODUCTION OF REGISTRATION REFUSAL REGISTRATION LIST BY EMD SERVICE CENTRE
S107 SAM OF RECEIVED ID NEWLY REGISTERED?
S114 PRODUCTION OF NEW REGISTRATION LIST BY EMD SERVICE CENTRE
S108 PRODUCTION OF UPDATED REGISTRATION LIST BY EMD SERVICE CENTRE
S109 TRANSMISSION OF DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY TO SAM BY EMD SERVICE CENTRE
S110 DECRYPTION AND STORAGE OF RECEIVED DELIVERY KEY BY SAM
S111 TRANSMISSION OF REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE
S112 DECRYPTION AND STORAGE OF RECEIVED REGISTRATION LIST BY SAM
RETURN

[FIG. 39]

START SAM STORAGE DATA BACKUP
S121 CROSS-AUTHENTICATION WITH IC CARD BY SAM
S122 GENERATION OF RANDOM NUMBER FOR USE AS BACKUP KEY
S123 ENCRYPTION OF SAM STORAGE DATA WITH BACKUP KEY
S124 ENCRYPTION OF BACKUP KEY WITH PUBLIC KEY OF EMD SERVICE CENTRE
S125 STORAGE OF ENCRYPTED SAME STORAGE DATA AND ENCRYPTED BACKUP KEY IN IC CARD
END

[FIG. 41]

START BACKUP READ PROCESSING TO NEW RECEIVER
S141 CROSS-AUTHENTICATION WITH IC CARD BY SAM
S142 READING ENCRYPTED SAM STORAGE DATA AND ENCRYPTED BACKUP KEY FROM IC CARD
S143 CROSS-AUTHENTICATION WITH EMD SERVICE CENTRE BY SAM
S144 TRANSMISSION OF ENCRYPTED SAM STORAGE DATA AND ENCRYPTED BACKUP KEY TO EMD SERVICE CENTRE BY SAM
S145 DECRYPTION OF BACKUP KEY WITH SECRET KEY BY EMD SERVICE CENTRE
S146 DECRYPTION OF SAM STORAGE DATA WITH BACKUP KEY BY EMD SERVICE CENTRE
S147 ENCRYPTION OF SAM STORAGE DATA WITH TEMPORARY KEY BY EMD SERVICE CENTRE
S148 TRANSMISSION OF SAM STORAGE DATA BY EMD SERVICE CENTRE
S149 DECRYPTION AND STORAGE OF RECEIVED DATA BY SAM
S150 SETTING PREVIOUS SAM ID AS UNREGISTERED BY EMD SERVICE CENTRE
RETURN

[FIG. 42]

START BACKUP READ PROCESSING TO NEW RECEIVER
S161 CROSS-AUTHENTICATION WITH IC CARD BY SAM
S162 READING ENCRYPTED SAM STORAGE DATA FROM IC CARD
S163 CROSS-AUTHENTICATION WITH EMD SERVICE CENTRE BY SAM
S164 TRANSMISSION OF ENCRYPTED SAM STORAGE DATA TO EMD SERVICE CENTRE BY SAM
S165 DECRYPTION OF SAM STORAGE DATA WITH SECRET KEY BY EMD SERVICE CENTRE
S166 ENCRYPTION OF SAM STORAGE DATA WITH TEMPORARY KEY BY EMD SERVICE CENTRE
S167 TRANSMISSION OF SAM STORAGE DATA BY EMD SERVICE CENTRE
S168 ENCRYPTION AND STORAGE OF RECEIVED DATA BY SAM
S169 SETTING PREVIOUS SAM ID AS UNREGISTERED BY EMD SERVICE CENTRE
RETURN

[FIG. 46]

START SECURE CONTAINER TRANSMISSION PROCESSING TO SERVICE PROVIDER

S251 INSERTION OF WATERMARK IN CONTENT

S252 COMPRESSION OF CONTENT

S253 GENERATION OF RANDOM NUMBER FOR USE AS CONTENT KEY

S254 ENCRYPTION OF CONTENT WITH CONTENT KEY

S255 ENCRYPTION OF CONTENT WITH DELIVERY KEY

S256 PRODUCTION OF SIGNATURE

S257 PRODUCTION OF SECURE CONTAINER

S258 CROSS-AUTHENTICATION WITH SERVICE PROVIDER

S259 TRANSMISSION OF SECURE CONTAINER

RETURN

[FIG. 44]

START RECEIVER DELIVERY KEY RECEIPT PROCESSING

S201 CROSS-AUTHENTICATION WITH EMD SERVER BY RECEIVER

S202 SEND AUTHENTICATION CERTIFICATE TO EMD SERVER BY RECEIVER

S203 HS RECEIVER UNREGISTERED?

S204 TRANSMISSION OF DELIVERY KEY VERSION, FEE CALCULATION USAGE POLICY AND REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY TO EMD SERVICE CENTRE BY RECEIVER

S205 DECRYPTION OF RECEIVED DATA AND FEE INFORMATION PROCESSING BY EMD SERVICE CENTRE

S206 IS DELIVERY KEY A NEW VERSION?

S207 TRANSMISSION OF REGISTRATION LIST AND FEE INFORMATION RECEIPT MESSAGE ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT AND DECRYPTION OF REGISTRATION LIST AND FEE CALCULATION RECEIPT MESSAGE BY RECEIVER

S208 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST BY RECEIVER

S209 TRANSMISSION OF REGISTRATION LIST, FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT AND DECRYPTION OF REGISTRATION LIST, FEE CALCULATION RECEIPT MESSAGE AND DELIVERY KEY BY RECEIVER

S210 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST AND DELIVERY KEY BY RECEIVER

RETURN

[FIG. 43]

START RECORDER REGISTRATION PROCESSING

S181 ADDITION OF RECORDER ID TO REGISTRATION LIST BY RECEIVER

S182 CROSS-AUTHENTICATION BETWEEN RECEIVER AND EMD SERVICE CENTRE

S183 IS RECEIVER REGISTERED?

S184 TRANSMISSION OF DELIVERY KEY VERSION, FEE INFORMATION, USAGE POLICY AND REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY TO THE EMD SERVICE CENTER BY RECEIVER

S185 DECRYPTION OF RECEIVED DATA, EXECUTION OF FEE PROCESSING AND UPDATE OF REGISTRATION LIST BY EMD SERVICE CENTRE

S186 IS RECEIVER DELIVERY KEY A REVISED VERSION?

S187 TRANSMISSION OF REGISTRATION LIST AND FEE INFORMATION RECEIPT MESSAGE ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT, DECRYPTION AND STORAGE OF REGISTRATION LIST AND FEE INFORMATION RECEIPT MESSAGE BY RECEIVER

S188 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST BY RECEIVER

S189 TRANSMISSION OF REGISTRATION LIST, FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT, DECRYPTION AND STORAGE OF REGISTRATION LIST, FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY BY RECEIVER

S190 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST AND DELIVERY KEY BY RECEIVER

S191 IS RECORDER UNREGISTERED?

S192 CROSS-AUTHENTICATION BETWEEN RECEIVER AND RECORDER

S193 TRANSMISSION OF REGISTRATION COMPLETION RECEIPT MESSAGE AND DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY BY RECEIVER, AND RECEIPT AND DECRYPTION OF REGISTRATION COMPLETION RECEIPT MESSAGE AND DELIVERY KEY BY RECORDER

S194 UPDATE OF DELIVERY KEY BY RECORDER

RETURN

[FIG. 45]

START RECORDER DELIVERY KEY RECEIPT

S221 CROSS-AUTHENTICATION BETWEEN RECEIVER AND RECORDER

S222 IS RECORDER LISTED ON RECEIVER REGISTRATION LIST?

S237 REGISTRATION OF RECORDER

S223 IS RECORDER UNREGISTERED?

S224 TRANSMISSION OF DELIVERY KEY VERSION AND FEE INFORMATION ENCRYPTED WITH TEMPORARY KEY TO THE RECEIVER BY RECORDER, AND RECEIPT OF DELIVERY KEY VERSION AND FEE INFORMATION BY RECEIVER

S225 CROSS-AUTHENTICATION BETWEEN RECEIVER AND EMD SERVICE CENTER

S226 IS RECEIVER UNREGISTERED?

S227 TRANSMISSION OF DELIVERY KEY VERSION, FEE INFORMATION, USAGE POLICY, REGISTRATION LIST OF RECEIVER AND FEE INFORMATION ENCYRPTED WITH A TEMPORARY KEY TO THE EMD SERVICE CENTRE BY THE RECEIVER

S228 DECRYPTION OF RECEIVED DATA AND EXECUTION OF FEE INFORMATION PROCESSING BY EMD SERVICE CENTRE

S229 IS RECEIVER DELIVERY KEY A REVISED VERSION?

S230 TRANSMISSION OF REGISTRATION LIST AND FEE INFORMATION RECEIPT MESSAGE ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT AND DECRYPTION OF REGISTRATION LIST AND FEE INFORMATION BY RECEIVER

S231 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST BY RECEIVER

S232 TRANSMISSION OF REGISTRATION LIST, FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY BY EMD SERVICE CENTRE, AND RECEIPT AND DECRYPTION OF REGISTRATION LIST, FEE INFORMATION AND DELIVERY KEY BY RECEIVER

S233 DELETION OF FEE INFORMATION AND UPDATE OF REGISTRATION LIST AND DELIVERY KEY BY RECEIVER

S234 IS RECORDER UNREGISTERED?

S235 TRANSMISSION OF FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY ENCRYPTED WITH TEMPORARY KEY BY RECEIVER, AND RECEIPT OF FEE INFORMATION RECEIPT MESSAGE AND DELIVERY KEY BY RECORDER

S236 DELETION OF FEE INFORMATION AND UPDATE OF DELIVERY KEY

RETURN

[FIG. 47]

START SECURE CONTAINER TRANSMISSION PROCESSING TO SERVICE PROVIDER
S271 INSERTION OF WATERMARK IN CONTENT
S272 COMPRESSION OF CONTENT
S273 GENERATION OF RANDOM NUMBER FOR USE AS CONTENT KEY
S274 ENCRYPTION OF CONTENT WITH CONTENT KEY
S275 ENCRYPTION OF CONTENT AND USAGE POLICY WITH DELIVERY KEY
S276 PRODUCTION OF SIGNATURE
S277 PRODUCTION OF SECURE CONTAINER
S278 CROSS-AUTHENTICATION WITH SERVICE PROVIDER
S279 TRANSMISSION OF SECURE CONTAINER
RETURN

[FIG. 48]

START SECURE CONTAINER TRANSMISSION PROCESSING TO RECEIVER
S291 EXTRACTION OF PUBLIC KEY FROM SECURE CONTAINER ACCY
S292 CONFIRMATION THAT THE SECURE CONTAINER HAS NOT BEEN FALSIFIED
S293 EXTRACTION OF USAGE POLICY FROM SECURE CONTAINER
S294 PRODUCTION OF PRICING INFORMATION
S295 PRODUCTION OF SECURE CONTAINER
S296 CROSS-AUTHENTICATION WITH RECEIVER
S297 TRANSMISSION OF SECURE CONTAINER
RETURN

[FIG. 49]

START SECURE CONTAINER TRANSMISSION PROCESSING TO RECEIVER
S311 EXTRACTION OF PUBLIC KEY FROM SECURE CONTAINER ACCY
S312 CONFIRMATION THAT THE SECURE CONTAINER HAS NOT BEEN FALSIFIED
S313 EXTRACTION OF SECURE CONTAINER USAGE POLICY
S314 PRODUCTION OF USAGE POLICY
S315 PRODUCTION OF PRICING INFORMATION
S316 PRODUCTION OF SECURE CONTAINER
S317 CROSS-AUTHENTICATION WITH RECEIVER
S318 TRANSMISSION OF SECURE CONTAINER
RETURN

[FIG. 51]

START REPRODUCTION PROCESSING
S361 EXTRACTION OF LICENSE USAGE CONDITIONS INFORMATION AND CONTENT KEY FROM HDD
S362 CALCULATION OF HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION
S363 MATCH WITH SAM HASH VALUE?
S378 ERROR PROCESSING
S364 UPDATE OF LICENSE USAGE CONDITIONS INFORMATION
S365 CALCULATION OF HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION
S366 STORAGE OF HASH VALUE IN SAM
S367 STORAGE OF LICENSE USAGE CONDITIONS INFORMATION IN HDD
S368 CROSS-AUTHENTICATION BETWEEN SAM AND EXPANDING PORTION, AND STORAGE OF TEMPORARY KEY
S369 DECRYPTION OF CONTENT KEY WITH SAVE KEY
S370 ENCRYPTION OF CONTENT KEY WITH TEMPORARY KEY
S371 SEND CONTENT KEY TO EXPANDING PORTION
S372 DECRYPTION OF CONTENT KEY WITH TEMPORARY KEY
S373 SEND CONTENT TO EXPANDING PORTION
S374 DECRYPTION OF CONTENT WITH CONTENT KEY
S375 EXPANSION OF CONTENT
S376 APPENDING WATERMARK TO CONTENT
S377 OUTPUT OF CONTENT
RETURN

[FIG. 50]

START FEE CALCULATION PROCESSING
S331 CAN CONTENT KEY BE DECRYPTED WITH DELIVERY KEY?
S332 DELIVERY KEY RECEIPT PROCESSING
S333 DECRYPTION OF CONTENT KEY WITH DELIVERY KEY
S334 GENERATION OF FEE INFORMATION AND LICENSE USAGE CONDITIONS FROM USAGE POLICY AND PRICING INFORMATION
S335 IS SUM OF CALCULATED FEES ABOVE UPPER LIMIT?
S336 DELIVERY KEY RECEIPT PROCESSING
S337 STORAGE OF FEE CALCULATING INFORMATION IN SAM
S338 RECORDING LICENSE USAGE CONDITIONS INFORMATION IN HDD
S339 RECORDING USAGE POLICY IN HDD
S340 CALCULATION OF HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION
S341 RECORDING HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION IN SAM
S342 GENERATION OF RANDOM NUMBER FOR USE AS SAVE KEY
S343 ENCRYPTING CONTENT KEY WITH SAVE KEY
S344 RECORDING CONTENT KEY IN HDD
S345 STORING SAVE KEY IN SAM
RETURN

[FIG. 52]

START REPRODUCTION PROCESSING
S391 EXTRACTION OF LICENSE USAGE CONDITIONS INFORMATION AND CONTENT KEY FROM HDD
S392 CALCULATION OF HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION
S393 MATCH WITH SAM HASH VALUE?
S408 ERROR PROCESSING
S394 UPDATE OF LICENSE USAGE CONDITIONS INFORMATION
S395 CALCULATION OF HASH VALUE OF LICENSE USAGE CONDITIONS INFORMATION
S396 STORAGE OF HASH VALUE IN SAM
S397 STORAGE OF LICENSE USAGE CONDITIONS INFORMATION IN HDD
S398 CROSS-AUTHENTICATION BETWEEN SAM AND EXPANDING PORTION, AND STORAGE OF TEMPORARY KEY
S399 DECRYPTION OF CONTENT KEY WITH SAVE KEY
S400 ENCRYPTION OF CONTENT KEY WITH TEMPORARY KEY
S401 SEND CONTENT KEY TO EXPANDING PORTION
S402 DECRYPTION OF CONTENT KEY WITH TEMPORARY KEY
S403 SEND CONTENT TO DECODER
S404 DECRYPTION OF CONTENT WITH CONTENT KEY
S405 EXPANSION OF CONTENT
S406 APPENDING WATERMARK TO CONTENT
S407 OUTPUT OF CONTENT
RETURN